AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 110–399

MODERNIZATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

TUESDAY, MAY 1, 2007

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

40–580 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

JOHN D. ROCKEFELLER IV, West Virginia, *Chairman*
CHRISTOPHER S. BOND, Missouri, *Vice Chairman*

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
EVAN BAYH, Indiana
BARBARA A. MIKULSKI, Maryland
RUSSELL D. FEINGOLD, Wisconsin
BILL NELSON, Florida
SHELDON WHITEHOUSE, Rhode Island

JOHN WARNER, Virginia
CHUCK HAGEL, Nebraska
SAXBY CHAMBLISS, Georgia
ORRIN HATCH, Utah
OLYMPIA J. SNOWE, Maine
RICHARD BURR, North Carolina

HARRY REID, Nevada, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
CARL LEVIN, Michigan, *Ex Officio*
JOHN MCCAIN, Arizona, *Ex Officio*

ANDREW W. JOHNSON, *Staff Director*
LOUIS B. TUCKER, *Minority Staff Director*
KATHLEEN P. MCGHEE, *Chief Clerk*

CONTENTS

Hearing held in Washington, DC:
May 1, 2007 1

Member Statements:

Rockefeller, Hon. John D. IV, Chairman, a U.S. Senator from West Virginia 1
Bond, Hon. Christopher S., Vice Chairman, a U.S. Senator from Missouri 4
Feingold, Hon. Russell D., a U.S. Senator from Wisconsin, prepared statement 51

Witness Statements:

McConnell, J. Michael, Admiral, USN, Ret., Director of National Intelligence 17
Prepared statement 7
Wainstein, Hon. Kenneth L., Assistant Attorney General, National Security Division, U.S. Department of Justice 45
Prepared statement 23

Statements for the Record:

Bankston, Kevin S., staff attorney, Electronic Frontier Foundation, prepared statement 73
Dempsey, James X., policy director, Center for Democracy and Technology, prepared statement 83
Fein, Bruce, prepared statement 98
Frederickson, Caroline, director, Washington Legislative Office, American Civil Liberties Union, prepared statement 104
Kris, David S., letter of response to government proposal 113
Martin, Kate, director, and Lisa Graves, deputy director, Center for National Security Studies, prepared statement 186
Spaulding, Suzanne E., prepared statement 207
Taipale, K.A., executive director, Center for Advanced Studies in Science and Technology Policy, prepared statement 218

MODERNIZATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

TUESDAY, MAY 1, 2007

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:35 p.m., in room SD–106, Dirksen Senate Office Building, the Honorable Jay Rockefeller, Chairman of the Committee, presiding.

Present: Senators Rockefeller, Feinstein, Wyden, Mikulski, Feingold, Nelson of Florida, Whitehouse, Levin, Bond, Warner, Hagel, and Snowe.

OPENING STATEMENT OF HON. JOHN D. ROCKEFELLER IV, CHAIRMAN, A U.S. SENATOR FROM WEST VIRGINIA

Chairman ROCKEFELLER. This hearing is begun, and I welcome all of our testifiers. Other members of the Committee will be coming in. I know some of the caucuses just broke up.

The Select Committee on Intelligence meets today in open session, something we don't often do, to consider whether the scope and application regarding the Surveillance Act needs to change to reflect the evolving needs for the timely collection of foreign intelligence. An extraordinarily complicated subject, this is.

At the Committee's request, the Administration has undertaken a comprehensive review of the Foreign Intelligence Surveillance Act, commonly referred to as FISA. Out of this review, the Administration proposed what it believes would modernize the laws governing the way in which we gather foreign intelligence with the use of electronic surveillance.

Our consideration of the Administration's proposal and alternatives will be rooted in the Intelligence Committee's 30-year experience with our Nation's long and delicate effort to strike that elusive right balance between effective intelligence collection for our national security and the constitutional rights and privacy interests of Americans.

The Intelligence Committee's existence came out of the work of the Church Committee and others in the mid-seventies to bring to light abuses in the electronic surveillance of Americans. One of the Committee's first tasks was to work with the Senate Judiciary Committee and with the Ford and Carter Administrations from 1976 to 1978 to enact the Foreign Intelligence Surveillance Act. As we take a fresh look at the current law, we will again be working with our colleagues in the Senate Judiciary Committee.

FISA involves both the judicial process on the one hand and the collection of intelligence. Our Committee's contribution to this process will be our ability to assess the relationship between the public realm of legislative reforms and the classified realm of intelligence collection. By necessity, much of the Committee's assessment must occur in a classified setting; yet while most of what we do, in contrast to the Judiciary Committee, will occur in closed session, I believe it is important to hold our hearing today in open session.

The purpose of today's hearing is to enable the Administration to explain to the Senate and to the American people as openly as possible the reasons why public law on these vital matters should be changed.

I would like to make a few observations about the Administration's legislative proposal before us.

One part of the Administration's bill proposes to terminate controversies now in litigation in various courts arising from the warrantless surveillance program that the President has labeled "the Terrorist Surveillance Program." It would bar any lawsuit against any person for the alleged provision to any element of the intelligence community information or assistance for any alleged communications intelligence activity.

Under the Administration's proposal, this immunity provision would be limited to alleged assistance from September 11, 2001, to 90 days after enactment of any change in the law, were there to be one. We will carefully examine this immunity process and proposal and possible alternatives to it—it is not without controversy—as we will all sections of the Administration bill. But I do believe that the Administration is going to have to do its part, too.

The Vice Chairman and I have stressed to the Administration repeatedly that the Committee must receive complete information about the President's surveillance program in order to consider legislation in this area. This is a matter of common sense. We cannot legislate in the blind. We have made some progress towards that end, but there are key pieces of requested information that the Committee needs and has not yet received.

These include the President's authorizations for the program and the Department of Justice's opinion on the legality of the program. My request for these documents is over a year in length, and Vice Chairman Bond and I restated the importance of receiving these documents in our March letter that in fact called this hearing. The Administration's delay in providing these basic documents is incomprehensible, I think, inexcusable, and serves only to hamper the Committee's ability to consider the liability defense proposal before it—inadequate information.

Congress is being asked to enact legislation that brings to end lawsuits that allege violations of the rights of Americans. In considering that request, it is essential that the Committee know whether all involved, government officials and anyone else, relied on sound, legal conclusions of the government's highest law officer. The opinions of the Attorney General are not just private advice. They are an authoritative statement of law within the Executive branch.

From our government's beginning in 1789 until 1982, there have been 43 published volumes of opinions of Attorneys General. Since then, there have been 24 published volumes of the opinions of DOJ's Office of Legal Counsel. From time to time, of necessity, a few will be classified. While those cannot be published, they can and should be provided to the congressional intelligence committees. We're in the classified business too, and we stick to it. There is simply no excuse for not providing to this Committee all of the legal opinions on the President's program.

The Administration's proposal to modernize FISA, if enacted, would be the most significant change to the statute since its enactment in 1978. It will be our duty to carefully scrutinize these proposed changes and ask many questions. And let me identify three.

First, from the beginning, FISA has required the approval of the FISA Court for the conduct of electronic surveillance done by wiretapping "in" the United States of America of communications "to or from" a person in the United States. The Judiciary Committee explained in its 1977 report to the Senate that this covers the wiretapping in the United States of the international communications of persons in the United States. The Administration would eliminate that requirement from the definition of electronic surveillance. An important question is whether that change will give the Attorney General authority, without a court warrant, to wiretap in the United States international communications that are to or from a person in the United States, most of whom will be United States citizens.

If so, what are the reasons for changing the judgment of the Congress in 1978 that a FISA order should be required for such wiretapping in the United States? How will that affect the private interests of U.S. citizens and permanent residents in their international communications?

Second, the Administration proposal would expand the power of the Attorney General to order the assistance of private parties without first obtaining a judicial FISA warrant that is based on the probable cause requirements in the present law. A limited form of judicial review will be available after those orders are issued. Although there are exceptions, our American legal tradition does not generally give our Attorney General the power to give such orders. Instead, it gives the Attorney General the power to go to the courts and ask for such orders. Is the Administration's proposal necessary, period? And does it take a step further down a path that we will regret as a nation?

Third, the Attorney General announced in January that the Administration had replaced the President's surveillance program with the orders of the FISA court. While many of my colleagues believe that the President's program should have been placed under court review and authorization much earlier, it was nonetheless good news. The question that we must now ask is whether, just months after that important development, any part of the Administration's bill will enable the President to resume warrantless collection with this legislation as the statutory basis for so doing.

Before turning to the Vice Chairman for his opening statement, I make a concluding remark or so. The Administration proposal was submitted to us by the Director of National Intelligence, Direc-

tor Mike McConnell, who will take the lead in presenting it to us today. The leadership of the DNI in this matter is a positive example of reform at work, and we welcome it.

General Keith Alexander, the Director of the National Security Agency, is representing the National Security Agency here today. The NSA, people should know, has a limited ability to speak for itself in public, but we can, the rest of us, and so I'd like to share this thought with my colleagues and with the American public.

NSA does not make the rules. It has no wish to do so. Congress sets policy for the NSA in law, and the President issues directives that the NSA must follow. Every American should have confidence, as we do from our close observation of this important truth, that the ranks of the NSA are filled with dedicated and honorable people who are committed to protecting this Nation while scrupulously following the laws and procedures designed to protect the rights and liberties of Americans.

Also on our panel is Keith Wainstein, the Assistant Attorney General for National Security. He is the first to hold that newly-created position. He has that for the first time. In our preparation for our hearing and other matters in recent months, we have been aided enormously by key personnel in his division as well as the Office of Legal Counsel.

Finally, the main purpose of today's hearing is to give the Administration a chance to place on the public record its proposal for change in public law. We also have invited interested members of the public, particularly individuals or organizations who have assisted the Congress from time to time with their views on FISA matters, to submit statements for our record about these legislative proposals.

I now turn to our distinguished Vice Chairman, Senator Bond.

OPENING STATEMENT OF HON. CHRISTOPHER S. BOND, VICE CHAIRMAN, A U.S. SENATOR FROM MISSOURI

Vice Chairman BOND. Thank you very much, Mr. Chairman. I join with you in welcoming the panelists and say how gratifying it is to see the intelligence community coming together working in a much more collaborative mood, an attitude that is very helpful.

We wish only that we could have the legislative structure that would facilitate such a cooperative working, and I join with you, having visited NSA, in paying the highest respect and regards to the work of the people at the NSA.

Since September 11, we've fought a myriad of enemies united in their ideological hatred of America—agile, widespread, technologically advanced. To prevail against them, our intelligence community needs tools that are flexible and can meet changing threats and circumstances. The purpose of today's hearing is to discuss whether the current statute provides enough flexibility and, if not, how do we update it.

Before I address serious aspects of the Administration's proposal, let me share some concerns about holding this particular hearing in a public setting before this Committee covers this issue behind closed doors.

The issue of FISA Modernization has come to the fore because of the very unfortunate public disclosure of the President's highly-

classified Terrorist Surveillance Program. Our Committee has been engaged in the oversight of the President's program since its inception, and now every member of this Committee, as I think they should, and an increased number of staff are read into the program, and we appreciate the clearance that has been expanded.

But as I've said before, the early warning system that is now under FISA is essential to defeating our enemies who are determined to inflict grave harm upon our citizens and upon the infrastructure of this Nation. I believe that having an open hearing before a closed hearing is not advisable, and I've given the Chairman recommendations in this regard.

Other Committees, like the Senate Judiciary Committee, have already considered aspects of this issue in open session because they were looking at it from a judicial point of view. Those members were not read in, for the most part, to the President's program. Our Committee looks at the issue from an intelligence and operational point of view, and our members therefore are read into the program.

There are several key reasons why I believe that proceeding first in open session is inadvisable.

First, this is an area where there is a very fine line between what is classified, sensitive or just shouldn't be highlighted in public.

Second, we've put witnesses before us in a bad position where they may be unable to respond to our question because the best responses are classified, including the best reasons to justify the new legislation they are proposing.

Third, although members of this Committee will go to a closed session and likely be satisfied with classified answers, the public may be left with the false impression that either the witnesses are not forthcoming or not fully answering our questions or even have good arguments. Worse yet, and with this topic in particular, if one of us were to make an honest mistake in wandering into sensitive territory, we could risk public exposure of vital intelligence collection methods that would significantly harm our intelligence capabilities.

Please don't misunderstand me, Mr. Chairman. I have confidence in our membership. However, I believe one of the reasons our Committee was created was to explore sensitive areas of national intelligence, to hash them out behind closed doors and to determine the best way to discuss them publicly, and then proceed with the public statements and report on them responsibly to the Senate with unclassified legislation.

And as the Chairman said, I believe that it is very important that there be a public discussion and I agree with the Chairman that that is a significant element. But I am troubled by proceeding first in public with a very sensitive national intelligence matter. I think we could serve our constituents and our national interests and the witnesses before us, ourselves and the American people if we had first proceeded in closed session. But that issue has been resolved.

I would caution, however, that all of us, Members and witnesses, will have to be especially diligent to ensure that questions and responses do not reveal any classified or sensitive information. And

we all share that responsibility. And I would encourage the witnesses that we understand you're not trying to be less than forthcoming if you reserve answers to a later closed session.

Turning now to the subject at hand, to examine the FISA statute, the Administration has offered some important suggestions and I expect that our witnesses will tell us why the changes are necessary and answer questions.

For instance, the Administration proposed to update the definition for the term "electronic surveillance" that will make it technology-neutral, unlike the current definition, which makes distinctions between wire, radio and other communications. The Administration proposal would modify the time period for emergency authorizations from 72 to 168 hours to ease the strain on vital resources within the Department of Justice and the FBI.

A long-overdue change is to update the FISA definition of the term "contents" to make it consistent with the definition used by the FISA pen register provision and the criminal wiretap statute. It simply makes no sense to have two different definitions for the same term in the same statute.

Another important improvement is to streamline FISA applications and orders. This streamlining would be consistent with one of the recommendations this Committee's staff audit made on the FISA project in 2005.

In summary, these are just some of the important issues we're going to discuss today. We must remember that change simply for change's sake is not the goal. Ensuring the collection capabilities of our intelligence community now and in the future should be the goal.

As we learned from the events of September 11, what we do here will have lasting effects not just on our intelligence sources and methods, but on our country's security.

Mr. Chairman, I'm sure that all of us look forward to a full and frank discussion about FISA modernization, the Administration's proposal, and the impact on our sources and methods. Our witnesses have considerable experience and credibility in matters of national security and intelligence, and I look forward to hearing their opinions.

I do understand the public interest in this subject, and I'll have some questions for the Administration during open session. However, as any full discussion will involve classified intelligence sources and methods, I would urge all my colleagues to exercise extra care in their questions and comments this afternoon.

With that, Mr. Chairman, I thank you for holding the hearing, and I look forward to hearing from our witnesses.

Chairman ROCKEFELLER. Thank you. I appreciate your comments very much, and I join you in always the concern of crossing the line. I do think it's important, however, that assuming that we can discipline ourselves not to cross the line, which I fully believe, I certainly know that you all can, and I certainly think that we can, that having this put before the American public in broad terms is useful, and then we go after it in a more vigorous way in closed session.

Having said that, Director McConnell, please proceed.

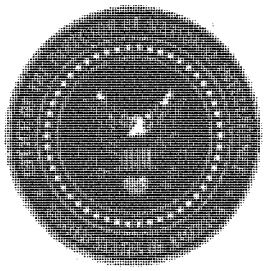
[The prepared statement of Director McConnell follows:]

Modernizing the Foreign Intelligence Surveillance Act

Statement for the Record

Senate Select Committee on Intelligence

May 1, 2007



J. Michael McConnell
Director of National Intelligence

Information as of
May 1, 2007

SENATE SELECT COMMITTEE ON INTELLIGENCE
FISA MODERNIZATION

UNCLASSIFIED
STATEMENT FOR THE RECORD

INTRODUCTION

Good morning Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee.

I am pleased to be here today in my role as the head of the Intelligence Community (IC) to express my strong support for the legislation that will modernize the Foreign Intelligence Surveillance Act of 1978 (FISA).

Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers and agents of foreign powers in the United States. My goal in appearing today is to share with you the critically important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the privacy rights of Americans.

The proposed legislation to amend FISA has several key characteristics:

- It makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978;
- It seeks to restore FISA to its original focus on protecting the privacy interests of persons in the United States;
- It enhances the Government's authority to secure assistance by private entities, which is vital to the IC's intelligence efforts;

- And, it makes changes that will streamline the FISA process so that the IC can use FISA as a tool to gather foreign intelligence information more quickly and efficiently.

As the Committee is aware, I have spent the majority of my professional life in the IC. In that capacity, I have been both a collector and a consumer, of intelligence information. I had the honor of serving as Director of the National Security Agency (NSA) from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function in enabling the collection of foreign intelligence information.

In my first eight weeks on the job as the new Director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. I cannot overstate how instrumental FISA has been in helping the IC protect the nation from terrorist attacks since September 11, 2001.

Some of the specifics that support my testimony cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose capability. I look forward to elaborating further on all aspects of the issues in a closed, classified setting.

I can, however, make a summary level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation.

TODAY'S NATIONAL SECURITY THREATS

Because I believe that the proposed legislation will advance our ability to protect the national security, I would like to take a few minutes to discuss some of the current threats. The most obvious is the continued threat from international terrorists. Despite the fact that we are in the sixth year following the attacks of September 11, 2001, and despite the steady progress we have made in dismantling the al Qaeda organization, significant threats from al Qaeda, other terrorist organizations aligned with it, and its sympathizers remain.

Today, America confronts a greater diversity of threats and challenges to attack inside our borders than ever before. As a result, the nation requires more from our IC than ever before.

I served as the Director of NSA at a time when the IC was first adapting to the new threats brought about by the end of the Cold War. Moreover, these new threats are enhanced by dramatic, global advances in telecommunications, transportation, technology, and new

centers of economic growth.

Although the aspects of Globalization are not themselves a threat, they facilitate terrorism, heighten the danger and spread of the proliferation of Weapons of Mass Destruction (WMD), and contribute to regional instability and reconfigurations of power and influence — especially through increasing competition for energy.

Globalization also exposes the United States to complex counterintelligence challenges. Our comparative advantage in some areas of technical intelligence, where we have been dominant in the past, is being eroded. Several non-state actors, including international terrorist groups, conduct intelligence activities as effectively as capable state intelligence services. Al Qaeda, and those aligned with and inspired by al Qaeda, continue to actively plot terrorist attacks against the United States, our interests and allies.

A significant number of states also conduct economic espionage. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects approaching Cold War levels.

FISA NEEDS TO BE TECHNOLOGY-NEUTRAL

In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs. Enacted nearly thirty years ago, it has not kept pace with 21st Century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S., i.e., foreign persons, located outside the United States. Currently, FISA forces a detailed examination of four questions:

Who is the target of the communications?
Where is the target located?
How do we intercept the communications?
Where do we intercept the communications?

This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing the FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.

The solution is to make the FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what changes technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Communications that, in 1978, would have been transmitted via radio or satellite, are transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain fiber optic cable transmissions currently fall under FISA's definition of electronic surveillance. Congress' intent on this issue is clearly stated in the legislative history:

"the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

Similarly, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, are included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

Today, IC agencies may apply, with the approval of the Attorney General and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the IC is often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of

a foreign person overseas.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order, based on a showing of probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: there are circumstances under which when the Government seeks to monitor, for purposes of protecting the nation from terrorist attack, the communications of **foreign** persons, who are physically located in **foreign** countries, the Government is required under FISA to obtain a court order to authorize this collection. We find ourselves in this position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

Moreover, this Committee and the American people should be confident that the information the IC is seeking is **foreign intelligence** information. Writ large, this includes information relating to the capabilities, intentions and activities of foreign powers, organizations or person, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets, while providing appropriate protection through court supervision to U.S. citizens and to other persons in the United States.

While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that FISA's regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. It is important to note that nothing in the proposed legislation changes this basic premise in the law.

Another thing that this proposed legislation does **not** do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States persons. For example, during the course of its normal business under current law, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities.

Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities that minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance

activities, and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence.

Some observers may be concerned about "reverse targeting" in which the target of the electronic surveillance is really a person in the United States who is in communication with the nominal foreign intelligence target overseas. In such cases, if the real target is in the United States, FISA would require the IC —to seek approval from the FISA Court in order to undertake such electronic surveillance.

In short, the FISA's definitions of "electronic surveillance" should be amended so that it no longer matters how collection occurs (whether off a wire or from the air). If the subject of foreign intelligence surveillance is a person reasonably believed to be in the United States or if all parties to a communication are reasonably believed to be in the United States, the Government should have to go to court to obtain an order authorizing such collection. If the government seeks to acquire communications of persons outside the United States, it will continue to be conducted under the lawful authority of Executive Order 12333, as they have been for decades.

SECURING ASSISTANCE UNDER FISA

The proposed legislation reflects that it is vitally important that the Government retain a means to secure the assistance of communications providers. As Director of NSA, a private sector consultant to the IC, and now Director of National Intelligence, I understand that in order to do our job, we frequently need the sustained assistance of those outside of government to accomplish our mission.

Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the Government with the exercise of **electronic surveillance** that is subject to Court approval under FISA. However, as a result of the proposed changes to the definition of electronic surveillance, FISA does not provide a comparable mechanism with respect to authorized **communications intelligence** activities. The proposal would fill this gap by providing the Government with means to obtain the aid of a court to ensure private sector cooperation with lawful intelligence activities.

This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private sector cooperation with activities that are "electronic surveillance" under current FISA, but that would no longer be if the definition were changed. It is equally critical that private entities that are alleged to have assisted the IC in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA

Modernization proposal contains a provision that would accomplish this objective.

THE FISA PROCESS SHOULD BE STREAMLINED

In addition to updating the statute to accommodate new technologies, protecting the rights of people in the United States, and securing the assistance of private parties, the proposed legislation also makes needed administrative changes. These changes include:

(1) streamlining applications made to the FISA Court, and (2) extending the time period the Department of Justice has to prepare applications following Attorney General authorized emergency collection of foreign intelligence information.

The Department of Justice estimates that these process-oriented changes potentially could save thousands of attorney work hours, freeing up the Justice Department's National Security lawyers and the FISA Court to spend more of their time and energy on cases involving United States persons - - precisely the cases we want them to be spending their efforts on. And, if we combine the streamlining provisions of this bill with the technology-oriented changes proposed, the Intelligence Community will be able to focus its operational personnel where they are needed most.

FISA WILL CONTINUE TO PROTECT CIVIL LIBERTIES

When discussing whether significant changes to FISA are appropriate, it is always appropriate to thoughtfully consider FISA's history. Indeed, the catalysts for FISA's enactment were abuses of electronic surveillance that were brought to light. The revelations of the Church and Pike committees resulted in new rules for U.S. intelligence agencies, rules meant to inhibit abuses while preserving our intelligence capabilities. I want to emphasize to this Committee, and to the American people, that none of the changes being proposed are intended to, nor will have the effect of, disrupting the foundation of credibility and legitimacy that FISA established.

Instead, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the Church and Pike investigations and the enactment of FISA. Following the adoption of FISA, a wide-ranging, new intelligence oversight structure was built into U.S. law. A series of laws and Executive Orders established oversight procedures and substantive limitations on intelligence activities. After FISA, the House and Senate each established intelligence oversight committees. Oversight mechanisms were established within the Department of Justice and within each intelligence agency – including a system of inspectors general.

More recently, additional protections have been implemented community-wide. The Privacy and Civil Liberties Oversight Board

was established by the Intelligence Reform and Terrorism Prevention Act of 2004. The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. Unlike in the 1970s, the IC today operates within detailed, constitutionally-based, substantive, and procedural limits under the watchful eyes of Congress, numerous institutions within the Executive Branch, and, through FISA, the judiciary.

With this robust oversight structure in place, it also is important to ensure that the IC is more effective in collecting and processing information to protect Americans from terrorism are other threats to the security of the United States. FISA must be updated to meet the new challenges faced by the IC.

The Congressional Joint Inquiry Commission into IC Activities Before and After the Terrorist Attacks of September 11, 2001, recognized that there were systemic problems with FISA implementation. For example, the Commission noted that "there were gaps in NSA's coverage of foreign communications and FBI's coverage of domestic communications." As a result of these and other reviews of the FISA process, the Department of Justice and IC have continually sought ways to improve.

The proposed changes to FISA address the problems noted by the Commission. At the same time, a concerted effort was made in our proposal to balance the country's need for foreign intelligence information with the need to protect core individual civil rights.

CONCLUSION

This proposed legislation seeks to accomplish several goals:

- First, the changes proposed are intended to make FISA technology-neutral, so that as communications technology develops - - which it absolutely will - - the language of the statute does not become obsolete.

- Second, this proposal is not intended to change privacy protections for Americans. In particular, this proposal makes no changes to the findings required to determine that a U.S. person is acting as an agent of a foreign power. The proposal returns the FISA to its original intent of protecting the privacy of persons in the United States.

- Third, the proposed legislation enhances the Government's ability to obtain vital assistance of private entities.

- And fourth, the proposed legislation allows the Government to make some administrative changes to the way FISA

applications are processed. As Congress has noted in its reviews of FISA process, streamlining the FISA process makes for better government.

This Committee should have confidence that we understand that amending FISA is a major proposal. We must get it right. This proposal is being made thoughtfully, and after extensive coordination for over a year.

Finally, I would like to state clearly my belief that bipartisan support for bringing FISA into the 21st Century is essential. Over the course of the last year, those working on this proposal have appeared at hearings before Congress, and have consulted with Congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the nation. I ask for your support in modernizing FISA so that it will continue to serve the nation for years to come.

As I stated before this Committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the nation's IC, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist activity and other threats to our security.

I look forward to answering the Committee's questions regarding this important proposal to bring FISA into the 21st Century.

STATEMENT OF ADMIRAL J. MICHAEL McCONNELL, USN, RET., DIRECTOR OF NATIONAL INTELLIGENCE ACCOMPANIED BY: LIEUTENANT GENERAL KEITH ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY; BENJAMIN A. POWELL, GENERAL COUNSEL, DIRECTOR OF NATIONAL INTELLIGENCE; VITO POTENZA, GENERAL COUNSEL, NATIONAL SECURITY AGENCY

Director McCONNELL. Good afternoon, Chairman Rockefeller, Vice Chairman Bond, members of the Committee. Thank you for inviting us to come today to engage with the Congress on legislation that will modernize the Foreign Intelligence Surveillance Act, as you mentioned, FISA—I'll refer to it as FISA from this point on—which was passed in 1978.

In response to your guidance from last year on the need to revise FISA, the Administration has worked for over the past year, with many of you and your staff experts, to craft the proposed legislative draft. It will help our intelligence professionals, if passed, protect the Nation by preventing terrorist acts inside the United States.

Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers or agents of foreign powers inside the United States. We are here today to share with you the critically important role that FISA plays in protecting the Nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the civil and the privacy rights of all Americans.

The proposed legislation to amend FISA has four key characteristics. First, it makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978. Second, it seeks to restore FISA to its original focus on protecting the privacy interests of persons inside the United States. Third, it enhances the government's authority to secure assistance by private entities, which is vital for the intelligence community to be successful. And fourth, it makes changes that will streamline FISA administrative processes so that the intelligence community can use FISA as a tool to gather foreign intelligence information more quickly and more effectively.

The four critical questions that we must address in collection against foreign powers or agents of foreign powers are the following. First, who is the target of the communications? Second, where is the target located? Third, how do we intercept the communications? And fourth, where do we intercept the communications? Where we intercept the communications has become a very important part of the determination that must be considered in updating FISA.

As the Committee is aware, I've spent the majority of my professional life in or serving the intelligence community. In that capacity, I've been both a collector of information and a consumer of intelligence information. I had the honor of serving as the Director of the National Security Agency from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function enabling the collection of foreign intelligence information.

In my first 10 weeks on the job as the new Director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. The threats faced by our Nation, as I have pre-

viously testified to this Committee, are very complex and they are very many. I cannot overstate how instrumental FISA has been in helping the intelligence community protect the Nation from terrorist attacks since September 11, 2001.

Some of the specifics that support my testimony, as has been mentioned, cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose the capability if known to the terrorists. I look forward to elaborating further on aspects of the issues in a closed session that is scheduled to follow.

I can, however, make the following summary-level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the intelligence community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.

Let me repeat that for emphasis. We are significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the Nation.

In today's threat environment, the FISA legislation is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S.—that is, foreign—persons located outside the United States.

Let me repeat again for emphasis. As a result, today's FISA requires judicial authorization to collect communications of non-U.S. persons—i.e., foreigners—located outside the United States. This clogs the FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail and before the Internet was a tool used by hundreds of millions of people worldwide every day.

There are two kinds of communications. It's important to just recapture the fact, two kinds of communications—wire and wireless. It's either on a wire—could be a copper wire, a fiber wire—it's on a wire or it's wireless, meaning it's transmitted through the atmosphere.

When the law was passed in 1978, almost all local calls were on a wire. Almost all local calls, meaning in the United States, were on a wire, and almost all long-haul communications were in the air, were known as wireless communications. Therefore, FISA in 1978 was written to distinguish between collection on a wire and collection out of the air or against wireless.

Now in the age of modern communications today, the situation is completely reversed. It's completely reversed. Most long-haul communications—think overseas—are on a wire—think fiberoptic

pipe. And local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA, passed in 1978. Technological advances have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act—and that is foreign-to-foreign communications by parties located overseas.

The solution is to make FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what technology may bring in the next 30 years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the Nation's security to a snapshot of outdated technology.

Additionally, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart. And yet simply because our law has not kept pace with technology, communications intended to be excluded from FISA are in fact included. This has real consequence on the intelligence community working to protect the Nation.

Today intelligence agencies may apply, with the approval of the Attorney General and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the intelligence community is often required to make a showing of probable cause.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the statutory requirement is to obtain a court order, based on a showing of probable cause; that slows, and in some cases prevents altogether, the government's effort to conduct surveillance of communications it believes are significant to national security, such as a terrorist coordinating attacks against the Nation located overseas.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly, when seeking to monitor foreign persons suspected of involvement in terrorist activity who are physically located in foreign countries, the intelligence community is required under today's FISA to obtain a court order to conduct surveillance. We find ourselves in a position, because of the language in the 1978 FISA statute, simply—we have not kept pace with the revolution in communications technology that allows the flexibility we need.

As stated earlier, this Committee and the American people should know that the information we are seeking is foreign intelligence information. Specifically, this includes information relating to the capabilities, intentions and activities of foreign powers or agents of foreign powers, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets while providing appropriate protection through court supervision to U.S. citizens and other persons located inside the United States.

Debates concerning the extent of the President's constitutional powers were heated in the mid-seventies, as indeed they are today. We believe that the judgment of the Congress at that time was that the FISA regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. Nothing—and I would repeat—nothing in the proposed legislation changes this basic premise in the law.

Additionally, this proposed legislation does not change the law or procedures governing how NSA or any other government agency treats information concerning U.S. or United States persons. For example, during the course of normal business under current law, NSA will sometimes—and I repeat—sometimes encounter information to, from or about a U.S. person; yet this fact does not in itself cause FISA to apply to NSA's overseas surveillance activities.

Instead, at all times, NSA applies procedures approved by the Attorney General to minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure constitutional reasonableness of NSA's surveillance activities.

They eliminate from intelligence reports incidentally-acquired information concerning U.S. persons that does not constitute foreign intelligence. The information is not targeted, stored, retained or used by the intelligence community.

Some observers may be concerned about reverse targeting. This could occur when a target of electronic surveillance is really a person inside the United States who is in communication with the nominal foreign intelligence target located overseas. In such cases, if the real target is in the United States, the intelligence community would and should be required to seek approval from the FISA Court in order undertake such electronic surveillance.

It is vitally important, as the proposed legislation reflects, that the government retain a means to secure the assistance of communications providers. As Director of NSA, a private-sector consultant both to government and to industry, and as now the Director of National Intelligence, I understand that it is in our interest and our job to provide the necessary support. To do that, we frequently need the sustained assistance of those outside the government to accomplish our mission.

Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the government to exercise electronic surveillance that is subject to court approval under FISA. However, the current FISA does not provide a comparable mechanism with respect to authorized communications intelligence activity. I'm differentiating between electronic surveillance and communications intelligence. The new legislative proposal would fill these gaps by providing the government with means to obtain the aid of a court to ensure private-sector cooperation with lawful intelligence activities and ensure protection of the private sector.

This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private-sector cooperation with the activities that are "electronic surveillance" under the current FISA, but that would no longer be if the defini-

tion were changed. It is equally critical that private entities that are alleged to have assisted the intelligence community in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA modernization proposal contains a provision that would accomplish this objective.

When discussing whether significant changes to FISA are appropriate, it is useful to consider FISA's long history. Indeed, the catalysts of FISA's enactment were abuses of electronic surveillance that were brought to light in the mid-seventies.

The revelations of the Church and Pike Committees resulted in new rules for United States intelligence agencies, rules meant to inhibit abuses while providing and protecting and allowing our intelligence capabilities to protect the Nation.

I want to emphasize to this Committee and to the American public that none of these changes, none of those being proposed, are intended to nor will they have the effect of disrupting the foundation of credibility and legitimacy of the FISA court, as established in 1978. Indeed, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the 1978 Church-Pike investigations and the enactment of the original FISA Act.

Following the adoption of FISA, a wide-ranging new oversight structure was built into U.S. law. A series of laws and executive office orders established oversight procedures and substantive limitations on intelligence activities, appropriately so.

After FISA, this Committee and its House counterpart were created. Oversight mechanisms were established within the Department of Justice and within each intelligence agency, including a system of inspectors general. More recently, additional protections have been implemented community-wide.

The Privacy and Civil Liberties Oversight Board was established by the Intelligence Reform and Terrorism Prevention Act of 2004. This board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations and Executive branch policies related to efforts to protect the Nation against terrorism.

Unlike in the 1970s, the intelligence community today operates with detailed, constitutionally-based, substantive and procedural limits under the watchful eyes of this Congress, numerous institutions within the Executive branch and, through FISA, the judiciary.

The Judicial Joint Inquiry Commission into Intelligence Activities Before and After the Terrorist Attacks of September 11, 2001, recognized that there were systematic problems with FISA implementation. For example, the Commission noted that "there were gaps in NSA's coverage of foreign communications and in FBI's coverage of domestic communications."

As a result of these and other reviews of the FISA process, the Department of Justice and the intelligence community have continually sought ways to improve. The proposed changes to FISA address the problems noted by that Commission.

Mr. Chairman, we understand that amending FISA is a major proposal. We must get it right. This proposal is being made

thoughtfully and after extensive coordination for over a year. But for this work to succeed, there must be bipartisan support for bringing FISA into the 21st century.

Over the course of the last year, those working on this proposal have appeared at hearings before Congress and have consulted with congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the Nation. I ask for your support in modernizing FISA so that we may continue to serve the Nation for years to come.

As I stated before this Committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the Nation's intelligence community, it is not only my desire but my duty to encourage changes to policies and procedures and, where needed, legislation to improve our ability to provide warning of terrorist activity and other threats to the Nation. I look forward to answering the Committee's questions regarding this important proposal to bring FISA into the 21st century.

Chairman ROCKEFELLER. Thank you, Mr. Director. That was forthright and informative, and we appreciate it.

Mr. Wainstein.

[The prepared statement of Mr. Wainstein follows:]

Department of Justice

STATEMENT OF

KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE
UNITED STATES SENATE

CONCERNING

THE NEED TO BRING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT
INTO THE MODERN ERA

PRESENTED

May 1, 2007

STATEMENT OF
KENNETH L. WAINSTEIN
ASSISTANT ATTORNEY GENERAL
NATIONAL SECURITY DIVISION
DEPARTMENT OF JUSTICE

CONCERNING

THE NEED TO BRING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT INTO THE MODERN ERA

BEFORE THE

SENATE SELECT COMMITTEE ON INTELLIGENCE

MAY 1, 2007

Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee, I want to thank you for this opportunity to testify in a public setting concerning the Administration's proposal to modernize the Foreign Intelligence Surveillance Act of 1978 (more commonly referred to as "FISA").

In order to explain why we must modernize FISA today, it is important to understand what Congress intended to accomplish when it drafted FISA almost thirty years ago. I will therefore begin my testimony today with a brief discussion of the context in which FISA was enacted. Then I will explain how sweeping changes since 1978—both in the nature of the threat that we face and in telecommunications technologies—have upset the delicate balance that Congress sought to achieve when it enacted FISA. As a result of these changes, FISA now regulates many intelligence activities of the sort that Congress sought to exclude from the scope of FISA—an unintended consequence that has impaired our intelligence capabilities. I will conclude by providing the Committee a detailed, but unclassified, explanation of the specific reforms of the statute that we believe are needed to restore FISA to its original focus. By

modernizing and streamlining FISA, we can improve our efforts to gather intelligence on those who seek to harm us, and do so in a manner that protects the civil liberties of Americans.

The FISA Congress Intended: The Scope of FISA in 1978

Congress enacted FISA in 1978 for the purpose of establishing a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."[1] The legislation came on the heels of the Church Committee Report, which disclosed abuses of domestic national security surveillances, and reflected a judgment that the civil liberties of Americans would be well-served by the development of a process for court approval of foreign intelligence surveillance activities directed at individuals in the United States. To accomplish this objective, Congress authorized the Attorney General to make an application to a newly established court—the Foreign Intelligence Surveillance Court (or "FISA Court")—seeking a court order approving the use of "electronic surveillance" against foreign powers or their agents.

However, in making these changes, Congress recognized the importance of striking an appropriate balance between the need to protect the civil liberties of Americans, and the imperative that the Government be able to collect effectively foreign intelligence information that is vital to the national security.[2] It also recognized that the terrain in which it was legislating touched upon a core Executive Branch function—the Executive's constitutional responsibility to protect the United States from foreign threats.[3] Congress attempted to accommodate these potentially competing concerns by applying FISA's process of judicial approval to certain

---

[1] H.R. Rep. No. 95-1283, pt. 1, at 22 (1978).
[2] *Id.* at 21, 22, 25.
[3] *See, e.g.*, *id.* at 15 (referring to "the President's constitutional powers to gather intelligence deemed necessary to the security of the nation").

intelligence activities (almost all of which occur within the United States), while excluding from FISA's regime of court supervision the vast majority of overseas foreign intelligence surveillance activities, including most surveillance focused on foreign targets. The intent of Congress generally to exclude these intelligence activities from FISA's reach is expressed clearly in the House Permanent Select Committee on Intelligence's report, which explained: "[t]he committee has explored the feasibility of broadening this legislation to apply overseas, but has concluded that certain problems and unique characteristics involved in overseas surveillance preclude the simple extension of this bill to overseas surveillances."[4]

The mechanism by which Congress gave effect to this intent was its careful definition of "electronic surveillance," the term that identifies which government activities fall within FISA's scope. This statutory definition is complicated and difficult to parse, in part because it defines "electronic surveillance" by reference to particular communications technologies that were in place in 1978. (Indeed, as will be explained shortly, it is precisely FISA's use of technology-dependent provisions that has caused FISA to apply to activities today that we submit its drafters never intended.) The fact that many of the intelligence activities at issue are highly classified further complicates any effort to explain these provisions in an unclassified setting.

By reading the plain text of these provisions in light of the telecommunications communications technologies available at the time of FISA's passage, however, we can learn a great deal both about what Congress intended to cover and about what intelligence activities it intended to exclude from FISA. Consider at the outset the first definition of electronic surveillance, which encompasses the acquisition of "the contents of any wire or radio communication sent by or intended to be received by *a particular, known United States person who is in the United States*, if the contents are acquired by intentionally targeting that United

[4] *Id.* at 27.

States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[5] In other words, if the Government intentionally targets a particular, known U.S. person in the United States for foreign intelligence purposes, it is within FISA's scope, period.

A close reading of FISA's definition of "electronic surveillance" in context makes a related point clear: if the Government directed surveillance at the communications of a person overseas, those acquisitions were generally excluded from FISA's scope. The key here is the third definition of electronic surveillance, which encompasses the acquisition of "radio communications" if "both the sender and all intended recipients are in the United States."[6] In 1978, almost all transoceanic communications into and out of the United States were radio communications carried by satellite. Accordingly, when FISA was enacted, the acquisition of most international communications would become "electronic surveillance" only if either (i) the acquisition intentionally targeted a U.S. person in the United States (in which case the acquisition would have fallen within the scope of the first definition, discussed above); or (ii) *all* of the participants to the communication were located in the United States (in which case the acquisition would fall within the third definition).[7] Therefore, in 1978, if the government acquired communications by targeting a foreign person overseas, it usually was not engaged in "electronic surveillance"—a result consistent with Congress's expressed intent, discussed above, to carve out most overseas intelligence activities.

---

[5] 50 U.S.C. 1801(f)(1).
[6] 50 U.S.C. 1801(f)(1).
[7] At the time of FISA's enactment, the remaining two definitions of "electronic surveillance" did not implicate most transoceanic communications. The first of these definitions, in section 1801(f)(2), applied only to "wire communications," which in 1978 carried a comparatively small number of transoceanic communications. The second definition, in section 1801(f)(4), was a residual definition that FISA's drafters explained was "not meant to include . . . the acquisition of those international radio transmissions which are not acquired by targeting a particular U.S. person in the United States." H.R. Rep. No. 95-1283 at 52.

It is important to note, however, that Congress created this carve-out by using the manner in which communications are transmitted as a proxy for the types of targets and communications that the statute intended to reach. As discussed below, this technology-dependent approach has had dramatic unintended consequences and has resulted in sweeping into FISA a wide range of intelligence activities that Congress intended to exclude from FISA in 1978. And FISA's use of technology-dependent language is not limited to these core definitions of "electronic surveillance." The distinction between "wire" and "radio" communications runs throughout the statute, and the statute also contains a provision authorizing the acquisition of communications "transmitted by means of communications used exclusively between or among foreign powers" that was premised upon the telecommunications technologies of the 1970s.

In addition to reflecting the technology of the time, the Act's legislative history also shows that the world was a different place when FISA was enacted. In terms of civil liberties, one of Congress's primary concerns was preventing the improper collection and dissemination of information about Americans involved in the civil rights movement and political activities.[8] In terms of threats, Congress was, in large part, concerned with espionage by agents of the Soviet Union.[9] The United States had not yet confronted the perils of large-scale international terrorism within the homeland,[10] and the faces of terrorism were groups such as Black September, the Baader-Meinhof Group, and the Japanese Red Army.[11] It was a time when Congress was worried that, if a terrorist hijacked an airplane, the purpose would be "to force the government to release a certain class of prisoners or to suspend aid to a particular country"[12] – not murder 3,000

[8] *See, e.g.*, S. Rep. No. 95-701, at 19, 23, 26.
[9] *Id.* at 14.
[10] H.R. Rep. No. 95-1283, at 30.
[11] *Id.*
[12] *Id.* at 45; S. Rpt. 95-701, at 23-24.

innocent men, women, and children. Congress could not have foreseen international terrorism on a scale that amounts to armed conflict.

The FISA We Have Today: The Unintended Consequences of Technological Change

As this Committee is aware, there have been revolutions in telecommunications technology since 1978. For example, when FISA was enacted, almost all local calls were carried on a wire and almost all transoceanic communications were radio communications. Today that situation is almost precisely reversed, as most long-haul communications are on a wire and local calls often travel by air. And of course, today we have wholly new methods of communicating—such as cell phones and e-mail—that either did not exist or were not in popular use in 1978. The drafters of the FISA did not and could not have anticipated these developments.

These unanticipated advances in technology have wreaked havoc on the delicate balance that Congress originally struck when it enacted FISA. Most importantly, those advances have largely upended FISA's intended carve-out of intelligence activities directed at persons overseas. As a result, the scope of FISA has been expanded radically, without any conscious choice by the Congress, to encompass a wide range of activities that FISA did not cover in 1978.

While a thorough description of these consequences can be discussed only in a classified session, I can state the bottom line here: considerable resources of the Executive Branch and the FISA Court are now expended on obtaining court orders to monitor the communications of terrorist suspects overseas. I believe most Americans would be surprised and dismayed to discover that America's intelligence agencies routinely use scarce resources to make a showing of probable cause, a notion derived from the Fourth Amendment, and obtain a court order before

acquiring the communications of these individuals. To make matters worse, these individuals frequently are communicating with other persons outside the United States. In certain cases, this process of obtaining a court order slows, and in some cases may prevent, the Government's efforts to conduct surveillance of communications that are potentially vital to the national security.

This unintended expansion of FISA's scope has hampered our intelligence capabilities and has caused us to expend resources on obtaining court approval to conduct intelligence activities directed at foreign persons overseas. This expansion of FISA's reach has necessarily diverted resources that would be better spent on protecting the privacy interests of United States persons here in the United States.

What We Should Do

We can and should amend FISA to restore its original focus on foreign intelligence activities that substantially implicate the privacy interests of individuals in the United States. The best way to restore that focus (and to reinstate the original carve-out for surveillance directed at foreign persons overseas) is to redefine the term "electronic surveillance" in a technology-neutral manner. Rather than focusing, as FISA does today, on *how* a communication travels or *where* it is intercepted, we should define FISA's scope by reference to *who is the subject of the surveillance.* If the surveillance is directed at a person in the United States, FISA generally should apply; if the surveillance is directed at persons overseas, it shouldn't. This would provide the Intelligence Community with much needed speed and agility while, at the

same time, refocusing FISA's privacy protections on United States persons located in the United States.

Some have suggested that the balance struck by Congress in 1978 did not go far enough; these critics argue that the Intelligence Community should be required to seek FISA Court approval each time a foreign target overseas happens to communicate with a person inside the United States. For reasons that I can elaborate upon in greater detail in closed session, this is an infeasible approach that would impose intolerable burdens on our intelligence efforts. As this Committee is aware, the Intelligence Community employs careful and thorough minimization procedures to handle the acquisition, dissemination, and retention of such incidentally collected U.S. person information. As Congress recognized in 1978, these rigorous procedures are a far more workable approach to protecting the privacy interests of Americans communicating with a foreign target than a sweeping new regime of judicial supervision for foreign intelligence surveillance activities targeting foreign persons overseas.

In addition to this critical change in the definition of "electronic surveillance," the Administration's proposal—which draws from a number of thoughtful bills introduced in Congress during its last session—also would make several other salutary changes to FISA. While I explain these in greater detail below, I will briefly summarize a few of the core changes here. First, it would amend the statutory definition of "agent of a foreign power" – a category of individuals the government may target under FISA – to include any person other than a U.S. person who possesses or is expected to transmit or receive foreign intelligence information within the United States. Second, the bill would fill a gap in our laws by permitting the Government to direct communications companies to assist in the conduct of lawful communications intelligence activities that do not constitute "electronic surveillance" under

FISA, and ensuring that they are protected from liability for having assisted the government in its counterterrorism efforts. Third, the bill would streamline the FISA application process in a manner that will make FISA more efficient, while at the same time ensuring that the FISA Court has the essential information it needs to evaluate a FISA application. The other sections of the proposal, all of which are detailed below, work in concert with these provisions to ensure our security while preserving the civil liberties of Americans.

Before I explain each section of the proposal, I would like to address one other theme that has arisen regarding FISA modernization. Some have suggested that amending FISA is unnecessary, either because Congress has modified FISA several times since September 11th, or because they believe that increased resources could address any problems with the statute. Congress has acted wisely in making several changes to FISA that were necessary and which improved the security of our nation. However, to address our shared goal of detecting and preventing another terrorist attack, we submit that it also is necessary to update the framework governing foreign intelligence surveillance to reflect today's very different telecommunications technologies and threats. Likewise, although additional resources are always welcome, committing even substantial additional funds and other resources would not solve all of the problems posed by the current FISA framework. We should restore FISA to its original focus on establishing a framework for judicial approval of the interception of communications that substantially implicate the privacy interests of individuals in the United States; changes at the margins will not enable us to achieve this goal.

Section by Section Analysis

For purposes of providing a complete review of the proposed legislation, the following is a short summary of each proposed change in the bill – both major and minor.

Section 401

Section 401 would amend several of FISA's definitions to address the consequences of the changes in technology that I have discussed. Most importantly, subsection 401(b) would redefine the term "electronic surveillance" in a technology-neutral manner that would refocus FISA on the communications of individuals in the United States As detailed above, when FISA was enacted in 1978, Congress used language that was technology-dependent and related specifically to the telecommunications systems that existed at that time. As a result of revolutions in communications technology since 1978, and not any considered judgment of Congress, the current definition of "electronic surveillance" sweeps in surveillance activities that Congress actually intended to *exclude* from FISA's scope. In this manner, FISA now imposes an unintended burden on intelligence agencies to seek court approval for surveillance in circumstances outside the scope of Congress' original intent.

Legislators in 1978 should not have been expected to predict the future of global telecommunications, and neither should this Congress. A technology-neutral statute would prevent the type of unintended consequences we have seen and it would provide a lasting framework for electronic surveillance conducted for foreign intelligence purposes. Thus, FISA would no longer be subject to unforeseeable technological changes. We should not have to overhaul FISA each generation simply because technology has changed.

Subsection 401(b) of our proposal provides a new, technology-neutral definition of "electronic surveillance" focused on the core question of *who* is the subject of the surveillance, rather than on *how* or *where* the communication is intercepted. Under the amended definition, "electronic surveillance" would encompass: "(1) the installation or use of an electronic, mechanical, or other surveillance device for acquiring information by intentionally directing

surveillance at a particular, known person who is reasonably believed to be located within the United States under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; or (2) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, if both the sender and all intended recipients are reasonably believed to be located within the United States." Under this definition, FISA's scope would not be defined by substantively irrelevant criteria, such as the means by which a communication is transmitted, or the location where the communication is intercepted. Instead, the definition would focus FISA's scope—as we believe Congress intended when it enacted the law in 1978—on those intelligence activities that most substantially implicate the privacy interests of persons in the United States.

Section 401 would make changes to other definitions in FISA as well. In keeping with the preference for technological neutrality, we would eliminate the distinction between "wire" and "radio" communications that appears throughout the Act. Accordingly, the Administration's proposal would strike FISA's current definition of "wire communication," because reference to that term is unnecessary under the new, technology neutral definition of "electronic surveillance."

The proposal also would amend other definitions to address gaps in FISA's coverage. Subsection 401(a) would amend FISA's definition of "agent of a foreign power" to include non-United States persons who possess or receive significant foreign intelligence information while in the United States. This amendment would ensure that the United States Government can collect necessary information possessed by a non-United States person visiting the United States. The amendment would thereby improve the Intelligence Community's ability to collect valuable

foreign intelligence in circumstances where a non-United States person in the United States is known to the United States Government to possess valuable foreign intelligence information, but his relationship to a foreign power is unclear. I can provide examples of scenarios in which this gap is evident in a classified setting. It merits emphasis that the Government would still have to obtain approval from the FISA Court to conduct surveillance under these circumstances.

Section 401 also amends the definition of the term "minimization procedures." This is an amendment that would be necessary to give meaningful effect to a proposed amendment to 50 U.S.C. 1802(a), discussed in detail below. Finally, section 401 would make the FISA definition of the term "contents" consistent with the definition of "contents" as that term is used in Title III, which pertains to interception of communications in criminal investigations. The existence of different definitions of "contents" in the intelligence and law enforcement contexts is confusing to those who must implement the statute.

Section 402

Section 402 would accomplish several objectives. First, it would alter the circumstances in which the Attorney General can exercise his authority – present in FISA since its passage – to authorize electronic surveillance without a court order. Currently, subsection 102(a) of FISA allows the Attorney General to authorize electronic surveillance without a court order where the surveillance is "solely directed" at the acquisition of the contents of communications "transmitted by means of communications used *exclusively*" between or among certain types of traditional foreign powers. This exclusivity requirement was logical thirty years ago in light of the manner in which certain foreign powers communicated at that time. But the means by which these foreign powers communicate has changed over time, and these changes in communications technology have seriously eroded the applicability and utility of current section 102(a) of FISA.

As a consequence, the Government must generally seek FISA Court approval for the same sort of surveillance today.

It is important to note that the proposed amendment to this provision of FISA would not alter the types of "foreign powers" to which this authority applies. It still would apply only to foreign governments, factions of foreign nations (not substantially composed of United States persons), and entities openly acknowledged by a foreign government to be directed and controlled by a foreign government or governments. Moreover—and this is important when read in conjunction with the change to the definition of "minimization procedures" referenced in section 401—any communications involving United States persons that are intercepted under this provision still will be handled in accordance with minimization procedures that are equivalent to those that govern court-ordered collection.

Section 402 also would create new procedures (those proposed in new sections 102A and 102B) pursuant to which the Attorney General could authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States, under circumstances in which the acquisition does not constitute "electronic surveillance" under FISA. This is a critical change that works hand in glove with the new definition of "electronic surveillance" in section 401. FISA currently provides a mechanism for the Government to obtain a court order compelling communications companies to assist in conducting electronic surveillance. Because the proposed legislation would reduce the scope of the definition of "electronic surveillance," certain activities that previously were "electronic surveillance" under FISA would fall out of the statute's scope. This new provision would provide a mechanism for the Government to obtain the aid of a court to ensure private sector cooperation with these lawful intelligence activities no longer covered by the definition of "electronic surveillance." The new

section would also provide a means for third parties receiving such a directive to challenge the legality of that directive in court.

Section 403

Section 403 makes two relatively minor amendments to FISA. First, subsection 403(a) amends section 103(a) of FISA to provide that judges on the FISA Court shall be drawn from "at least seven" of the United States judicial circuits. The current requirement – that judges be drawn from seven different judicial circuits – unnecessarily complicates the designation of judges for that important court.

Subsection 403(b) also moves to section 103 of FISA, with minor amendments, a provision that currently appears in section 102. New section 103(g) would provide that applications for a court order under section 104 of FISA are authorized if the Attorney General approves the applications to the FISA Court, and a judge to whom the application is made may grant an order approving electronic surveillance in accordance with the statute—a provision that is most suitably placed in section 103 of FISA, which pertains to the FISA Court's jurisdiction. The new provision would eliminate the restriction on the FISA Court's jurisdiction in 50 U.S.C. § 1802(b), which provides that the court cannot grant an order approving electronic surveillance directed at the types of foreign powers described in section 102(a) unless the surveillance may involve the acquisition of communications of a United States person. Although the Government still would not be required to obtain FISA Court orders for surveillance involving those types of foreign powers, the removal of this restriction would permit the Government to seek FISA Court orders in those circumstances when an order is desirable.

Section 404

The current procedure for applying to the FISA Court for a surveillance order under section 104 of FISA should be streamlined. While FISA should require the government to provide information necessary to establish probable cause and other essential FISA requirements, FISA today requires the government to provide information that is not necessary to these objectives.

Section 404 would attempt to increase the efficiency of the FISA application process in several ways. First, the Government currently is required to provide significant amounts of information that serves little or no purpose in safeguarding civil liberties. By amending FISA to require only summary descriptions or statements of certain information, the burden imposed on applicants for a FISA Court order authorizing surveillance will be substantially reduced. For example, section 404 would amend the current FISA provision requiring that the application contain a "detailed description of the nature of the information sought," and would allow the government to submit a summary description of such information. Section 404 similarly would amend the current requirement that the application contain a "statement of facts concerning all previous applications" involving the target, and instead would permit the government to provide a summary of those facts. While these amendments would help streamline FISA by reducing the burden involved in providing the FISA Court with information that is not necessary to protect the privacy of U.S. persons in the United States, the FISA Court would still receive the information it needs in considering whether to authorize the surveillance.

Section 404 also would increase the number of individuals who can make FISA certifications. Currently, FISA requires that such certifications be made only by senior Executive Branch national security officials who have been confirmed by the Senate. The new

provision would allow certifications to be made by individuals specifically designated by the President and would remove the restriction that such individuals be Senate-confirmed. As this committee is aware, many intelligence agencies have an exceedingly small number of Senate-confirmed officials (sometimes only one, or even none), and the Administration's proposal would allow intelligence agencies to more expeditiously obtain certifications.

Section 405

Section 405 would amend the procedures for the issuance of an order under section 105 of FISA to conform with the changes to the application requirements that would be effected by changes to section 104 discussed above.

Section 405 also would extend the initial term of authorization for electronic surveillance of a non-United States person who is an agent of a foreign power from 120 days to one year. This change will reduce time spent preparing applications for renewals relating to non-United States persons, thereby allowing more resources to be devoted to cases involving United States persons. Section 405 would also allow any FISA order to be extended for a period of up to one year. This change would reduce the time spent preparing applications to renew FISA orders that already have been granted by the FISA Court, thereby increasing the resources focused on initial FISA applications.

Additionally, section 405 would make important amendments to the procedures by which the Executive Branch may initiate emergency authorizations of electronic surveillance prior to obtaining a court order. Currently the Executive Branch has 72 hours to obtain court approval after emergency surveillance is initially authorized by the Attorney General. The amendment would extend the emergency period to seven days. This change will help ensure that the Executive Branch has sufficient time in an emergency situation to accurately prepare an

application, obtain the required approvals of senior officials, apply for a court order, and satisfy the court that the application should be granted. This provision also would modify the existing provision that allows certain information to be retained when the FISA Court rejects an application to approve an emergency authorization. Presently, such information can be retained if it indicates a threat of death or serious bodily harm to any person. The proposed amendment would also permit such information to be retained if the information is "significant foreign intelligence information" that, while important to the security of the country, may not rise to the level of death or serious bodily harm.

Finally, section 405 would add a new paragraph that requires the FISA Court, when granting an application for electronic surveillance, to simultaneously authorize the installation and use of pen registers and trap and trace devices if such is requested by the Government. This is a technical amendment that results from the proposed change in the definition of "contents" in Title I of FISA. And, of course, as the standard to obtain a court order for electronic surveillance is substantially higher than the pen-register standard, there should be no objection to an order approving electronic surveillance that also encompasses pen register and trap and trace information.

Section 406

Section 406 would amend subsection 106(i) of FISA, which pertains to limitations regarding the use of unintentionally acquired information. Currently, subsection 106(i) provides that lawfully but unintentionally acquired *radio* communications between persons located in the United States must be destroyed unless the Attorney General determines that the communications indicate a threat of death or serious bodily harm. Section 406 amends subsection 106(i) by making it technology-neutral; we believe that the same rule should apply

regardless how the communication is transmitted. The amendment also would allow for the retention of unintentionally acquired information if it "contains significant foreign intelligence information." This ensures that the government can retain and act upon valuable foreign intelligence information that is collected unintentionally, rather than being required to destroy all such information that does not fall within the current exception.

Section 406 also would clarify that FISA does not preclude the government from seeking protective orders or asserting privileges ordinarily available to protect against the disclosure of classified information. This is necessary to clarify any ambiguity regarding the availability of such protective orders or privileges in litigation.

Section 407

Section 407 would amend sections 101, 106, and 305 of FISA to address concerns related to weapons of mass destruction. These amendments reflect the threat posed by these catastrophic weapons and would extend FISA to apply to individuals and groups engaged in the international proliferation of such weapons. Subsection 407(a) amends section 101 of FISA to include a definition of the term "weapon of mass destruction." Subsection 407(a) also amends the section 101 definitions of "foreign power" and "agent of a foreign power" to include groups and individuals (other than U.S. persons) engaged in the international proliferation of weapons of mass destruction. Subsection 407(a) similarly amends the definition of "foreign intelligence information." Finally, subsection 407(b) would amend sections 106 and 305 of FISA, which pertain to the use of information, to include information regarding the international proliferation of weapons of mass destruction.

Section 408

Section 408 would provide litigation protections to telecommunications companies who are alleged to have assisted the government with classified communications intelligence activities in the wake of the September 11th terrorist attacks. Telecommunications companies have faced numerous lawsuits as a result of their alleged activities in support of the government's efforts to prevent another terrorist attack. If private industry partners are alleged to cooperate with the Government to ensure our nation is protected against another attack, they should not be held liable for any assistance they are alleged to have provided.

Section 409

Section 409 would amend section 303 of FISA (50 U.S.C. 1823), which relates to physical searches, to streamline the application process, update and augment the emergency authorization provisions, and increase the potential number of officials who can certify FISA applications. These changes largely parallel those proposed to the electronic surveillance application process. For instance, they include amending the procedures for the emergency authorization of physical searches without a court order to allow the Executive Branch seven days to obtain court approval after the search is initially authorized by the Attorney General. Section 409 also would amend section 304 of FISA, pertaining to orders authorizing physical searches, to conform to the changes intended to streamline the application process.

Additionally, section 409 would permit the search of not only property that *is* owned, used, possessed by, or in transit to or from a foreign power or agent of a foreign power, but also property that is *about* to be owned, used, possessed by, or in transit to or from these powers or agents. This change makes the scope of FISA's physical search provisions coextensive with FISA's electronic surveillance provisions in this regard.

Section 410

Section 410 would amend the procedures found in section 403 of FISA (50 U.S.C. 1843) regarding the emergency use of pen registers and trap and trace devices without court approval to allow the Executive Branch seven days to obtain court approval after the emergency use is initially authorized by the Attorney General. (The current period is 48 hours.) This change would ensure the same flexibility for these techniques as would be available for electronic surveillance and physical searches.

Section 411

Section 411 would allow for the transfer of sensitive national security litigation to the FISA Court in certain circumstances. This provision would require a court to transfer a case to the FISA Court if: (1) the case is challenging the legality of a classified communications intelligence activity relating to a foreign threat, or the legality of any such activity is at issue in the case, and (2) the Attorney General files an affidavit under oath that the case should be transferred because further proceedings in the originating court would harm the national security of the United States. By providing for the transfer of such cases to the FISA Court, section 411 ensures that, if needed, judicial review may proceed before the court most familiar with communications intelligence activities and most practiced in safeguarding the type of national security information involved. Section 411 also provides that the decisions of the FISA Court in cases transferred under this provision would be subject to review by the FISA Court of Review and the Supreme Court of the United States.

Other Provisions

Section 412 would make technical and conforming amendments to sections 103, 105, 106, and 108 of FISA (50 U.S.C. 1803, 1805, 1806, 1808).

Section 413 provides that these amendments shall take effect 90 days after the date of enactment of the Act, and that orders in effect on that date shall remain in effect until the date of expiration. It would allow for a smooth transition after the proposed changes take effect.

Section 414 provides that any provision in sections 401 through 414 held to be invalid or unenforceable shall be construed so as to give it the maximum effect permitted by law, unless doing so results in a holding of utter invalidity or unenforceability, in which case the provision shall be deemed severable and shall not affect the remaining sections.

Conclusion

For reasons that could not have been anticipated by Congress in 1978, FISA no longer reflects the delicate balance that Congress intended to strike when it enacted the statute. Radical technological changes in telecommunications have resulted in a vast array of overseas intelligence activities that were originally excluded from FISA being swept within FISA's scope. The proposal that the Administration has submitted to the Congress would restore FISA to its original focus on the protection of the privacy interests of Americans—a change that would both improve our intelligence capabilities and ensure that scarce Executive Branch and judicial resources are devoted to the oversight of intelligence activities that most clearly implicate the privacy interests of Americans. We look forward to working with the Congress to achieve these critical goals.

Thank you for the opportunity to appear before you and testify in support of the Administration's proposal. I look forward to answering your questions.

STATEMENT OF KENNETH L. WAINSTEIN, ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. WAINSTEIN. Thank you. Chairman Rockefeller, Vice Chairman Bond and members of the Committee, I want to thank you for this opportunity to testify about our proposal to modernize FISA. My colleagues and I have been working closely with this Committee and your staff on this and several other FISA-related issues. And I want to express my appreciation on the part of all of us up here for your cooperative approach on these complicated and very important matters.

While the proposal before you today contains a number of important and needed improvements to the FISA process, I'd like to focus my opening statement on laying out the merits of one particular improvement that we're advocating, which is our proposal to revise the definition of electronic surveillance in the FISA statute. To do that I'll begin with a brief discussion of Congress's intent when it drafted FISA almost 30 years ago. I'll then address the sweeping changes in telecommunications technology that have caused the statute to deviate from its original purpose, so that it now covers many intelligence activities that Congress intended not to cover.

I will discuss how this unintended consequence has impaired our intelligence capabilities, and I'll urge you to modernize FISA to bring it back in line with its original purpose.

In enacting FISA back in 1978, Congress established a regime of judicial review and approval, and applied that regime to the government's foreign intelligence surveillance activities. But Congress applied that regime not as to all such activities, but only as to those that most substantially implicated the privacy interests of people in the United States. In defining the scope of the statute, Congress was sensitive to the importance of striking an appropriate balance between the protection of privacy on one hand and the collection of critical foreign intelligence information on the other.

Congress struck that balance by designing a process that focused primarily on intelligence collection activities within the United States, where privacy interests are the most pronounced, and not on intelligence collection activities outside the United States, where cognizable privacy interests are minimal or non-existent.

Congress gave effect to this purpose through its careful definition of the statutory term "electronic surveillance," which is the term that identifies those collection activities that fall within the scope of the statute and, by implication, those that fall outside of it. Congress established this dichotomy by defining electronic surveillance by reference to the manner of the communication under surveillance, by distinguishing between wire communications, which, as the Director said, were primarily the local and domestic traffic in 1978, and radio communications, which were primarily the international traffic of that era.

Based on the communications reality of that time, that dichotomy more or less accomplished the congressional purpose of distinguishing between domestic communications which fell within FISA, and communications targeted at persons overseas which did not.

That reality has changed, however. It has changed with the enormous changes in communications technology over the past 30 years. With the development of new communications over cellular telephones, the Internet, and other technologies that Congress did not anticipate and could not have anticipated back in 1978, the foreign domestic dichotomy that Congress built into the statute has broken down.

As a result of that, FISA now covers a wide range of foreign activities that it did not cover back in 1978, and, as a result of that, the Executive branch and the FISA Court are now required to spend a substantial share of their resources every year to apply for and process court orders for surveillance activities against terror suspects and terrorist associates who are located overseas—resources that would be far better spent protecting the privacy interests of persons here in the United States.

We believe this problem needs to be fixed, and we submit that we can best fix it by restoring FISA to its original purpose. And to do that, we propose redefining the term "electronic surveillance" in a technology-neutral manner. Rather than focusing, as FISA does today, on how a communication travels or where it is intercepted, we should define FISA's scope by who is the subject of the surveillance, which really is the critical issue for civil liberties purposes. If the surveillance is directed at a person in the United States, FISA generally should apply. If the surveillance is directed at a person outside the United States, it should not.

This would be a simple change, but it would be a critically important one. It would refocus FISA's primary protections right where they belong, which is on persons within the United States.

It would realign FISA and our FISA Court practice with the core purpose of the statute, which is the protection of the privacy interests of Americans inside America. And it would provide the men and women of the intelligence community with the legal clarity and the operational agility that we need to surveil potential terrorists who are overseas. Such a change would be a very significant step forward both for our national security and for our civil liberties.

I want to thank you, all the members of the Committee, for your willingness to consider this legislative proposal as well as the other proposals in the package that we submitted to Congress, and I stand ready to answer any questions that you might have.

Thank you.

Chairman ROCKEFELLER. Thank you, sir, very much. We appreciate that.

And as I understand it, Director McConnell, all the other members of the panel are available also to answer questions.

Director MCCONNELL. Yes, sir, that's correct.

Chairman ROCKEFELLER. If I might start, the Administration's proposed change to FISA would exempt any international communications in and out of the United States from requiring the review and approval of a FISA judge before the surveillance took place unless a U.S. person was the specific target of the surveillance. In other words, phone calls between foreign targets and Americans located in the U.S. could be intercepted without regard to whether a probable cause standard was demonstrated to the court. This change in law, if enacted, would increase the number of commu-

nications involving U.S. persons being intercepted without a court warrant, and that would be at unprecedented levels.

So my question, in a sense, is a little bit like what Mr. Wainstein was talking about. If you're targeting a foreign person—and I stay within bounds here, but if you're targeting a foreign person, you're also at the same time picking up a United States citizen. You're not just sort of picking up one and not the other. So I'm not sure how that protects the United States citizen, No. 1. I need to know that.

Secondly, what private safeguards are there in the Administration's bill for the communications of Americans who are not a target but whose communications would be otherwise legally intercepted under a bill, which is sort of the same question that I just asked. If the court does not play a role in reviewing the appropriateness of surveillance that may ensnare the international phone calls of Americans, who—under the Administration's proposal—would oversee those exempt communications to ensure that U.S. persons were not being targeted?

Director MCCONNELL. Sir, I have to——

Chairman ROCKEFELLER. Who watches?

Director MCCONNELL. Let me be careful in how I frame my answer, because I will quickly get into sources and methods that we would not desire those plotting against us, terrorists, to understand or know about.

But in the lead to your statement, where you said a person inside the United States calling out, in all cases that would be subject to a FISA authorization. In the context of intelligence, it would be a foreign power or an agent of foreign power, calling out.

Now, if a known terrorist calls in and we're targeting the known terrorist, and someone answers the telephone in the United States, we have to deal with that information.

Chairman ROCKEFELLER. And I understand that and don't disagree with that, in fact support that. But my question is, in the process of carrying that out, properly, because you have reason to believe, so to speak, nevertheless the U.S. citizen is being recorded and is a part of the record. And therefore is that person's privacy targeted or not, even if that person is not the purpose of the action?

Director MCCONNELL. The key is "target" and would not be a target of something we were attempting to do. And since FISA was enacted in 1978, we've had this situation to deal with on a regular basis.

Recall in my statement I said in those days most overseas communications were wireless. Americans can be using that overseas communications. So as a matter of due course, if you're targeting something foreign, you could inadvertently intercept an American.

The procedures that were established following FISA in 1978 are called minimize. There is an established rigorous process.

Chairman ROCKEFELLER. I understand.

Director MCCONNELL. And so that is how you would protect it.

Let me turn it over to General Alexander, who is more current than I am on specific detail.

General ALEXANDER. Sir, if I might, if you look at where on the network you intercept that call, if we were allowed to intercept that overseas without a warrant, we'd pick up the same call talking to a person in the U.S. In doing that, we have rules upon which we

have to abide to minimize the U.S. person's data that's handed down to us from the Attorney General. Everyone at NSA is trained on how to do that.

It would apply the same if that were done in the United States under the changes that we have proposed. So we have today a discrepancy on where we collect it.

And the second, as Director McConnell pointed out, the minimization procedures would be standard throughout the world on how we do it. If a U.S. person was intercepted, if it was overseas or in the States, in both cases we'd minimize it.

Chairman ROCKEFELLER. I will come back to that. My time is up, and I call on the distinguished Vice Chairman.

Vice Chairman BOND. I thank the distinguished Chairman.

And I think that, Mr. Chairman, that answer is one which we should fully develop in a closed session, because I think that there's lots more to be said about that. And I think that question will be a very interesting one to explore later.

I'd ask Admiral McConnell or General Alexander, without getting in any classified measures, can you give us some insight maybe, General, or a specific example how important FISA is to defending ourselves against those who have vowed to conduct terrorist attacks on us?

Director MCCONNELL. Sir, let me start for a general observation, and I want to compare when I left and when I came back. And then I'll turn it to General Alexander for specifics.

The way you've just framed your question, when I left in 1996, retired, it was not significant. It was almost insignificant. And today it is probably the most significant ability we have to target and be successful in preventing attacks.

General ALEXANDER. Sir, as Director McConnell said, it is the key to the war on terrorism. FISA is the key that helps us get there.

Having said that, there's a lot more that we could and should be doing to help protect and defend the Nation.

Director MCCONNELL. Senator, I just might add—since I'm coming back to speed and learning the issues and so on—what I'm amazed with is, under the construct today, the way the definitions have played out and applied because technology changes, we're actually missing a significant portion of what we should be gathering.

Vice Chairman BOND. I think probably we want to get into that later, but I guess in summary you would say that this—you said this is the most important tool, and the information that you've gained there has allowed us on a number of occasions to disrupt activities that would be very harmful abroad and here.

Is that a fair statement?

Director MCCONNELL. Inside and outside the United States.

Vice Chairman BOND. All right. Mr. Wainstein, the proposal includes a new definition for an agent of a foreign power who possesses foreign intelligence information.

Can you give us an example of the type of person this provision is intended to target, and how that meets the particularity and reasonableness requirement of the Fourth Amendment?

Mr. WAINSTEIN. Thank you, Senator. Speaking within the parameters of what we can talk about here in open session—and I think

that's a particular concern in this particular case, where identifying any example with great particularity could actually really tip off our adversaries—let me just sort of keep it in general terms. This new definition of an agent of foreign power would fill a gap in our coverage right now, which is that there are situations where a person, a non-U.S. person—this is only non-U.S. person—is here in the United States. That person possesses significant foreign intelligence information that we would want to get that could relate to the intent of foreign powers who might want to do us harm. But because we cannot connect that person to a particular foreign power—under the current formulation of agent of foreign power—we're not able to go to the FISA Court and get approval, get an order allowing us to surveil that person.

So, you know, keep in mind, this is a FISA Court order. We'd do this pursuant to the FISA Court's approval. This is intended to provide that—fill that gap, similar to what Congress did when it gave us the lone wolf provision a couple years ago, allowing us to target a terrorist whom we could not connect to a particular foreign power.

That's critically important, and I would ask if I could defer to a closed session——

Vice Chairman BOND. We'll finish that up.

Another broader question. The recent inspector general's report detailed too many errors in the FBI's accounting for and issuing national security letters. As a result, some have suggested that the national security letter authorities should be changed or limited. What impact would changing the standard from relevance to a higher standard have on FBI operations, particularly in obtaining FISA surveillance and search authorities?

Mr. POWELL. I don't know what numbers would be cut out if the standard were changed. I think it is important to note—and this Committee has available to it the classified inspector general report that goes into great detail of where NSLs have been used in specific cases to obtain very critical information to enable foreign intelligence investigations to go forward, so I think if the standard were changed, that would lead to a real impact on those investigations. But Mr. Wainstein is closer to those and may want to comment.

Mr. WAINSTEIN. I'll echo what Mr. Powell said. And I believe that the remedy or the way of addressing the failings—which were failings; it's been acknowledged as serious failings by the Director of the FBI and the Attorney General—is not to scale back on the authority but to make sure that that authority is well-applied. And there are many things in process right now to make sure that'll happen.

Vice Chairman BOND. Just follow the rules.

Thank you very much, Mr. Chairman.

Chairman ROCKEFELLER. Thank you, Vice Chairman Bond.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

Admiral, I very much appreciated our private conversations and discussion about how we balance this effort in terms of fighting terrorism ferociously and protecting privacy. And what I want to ex-

amine with you is, what's really going to change on the privacy side?

For example, in the debate about national security letters, when Congress expanded the authority to issue these letters to thousands of Americans, most of the very same terms were used then that have been used this afternoon, efforts, for example, such as minimizing the consequences of the law. But recently the Director of the FBI has admitted that there was widespread abuse of the national security letter authority, that there were instances when agents claimed emergency powers despite the lack of an actual emergency.

What is going to change now with this new effort, so that we don't have Administration officials coming, as the Attorney General recently did, to say, made a mistake—widespread abuse?

Director MCCONNELL. First of all, the proposal is privacy-neutral. It doesn't change anything. NSLs are not a part of FISA.

Senator WYDEN. I understand that. But what concerns me, Admiral, is, we were told exactly the same thing with national security letters. We asked the same questions. We were told that there would be efforts to minimize the consequences. And I want to know, what's going to be different now than when we were told there wouldn't be abuses in the national security letters?

Director MCCONNELL. Sir, let me separate the two, if I could. FISA grew out of abuses that occurred in the seventies, as I mentioned in my opening statement. As a result of that, the hearings that were held by this body with regard to how we administer it going forward, the intelligence community was given very strict guidance with regard to the law and the implementing instructions and so on. There are instructions, and I think if you check back in time, the signature on the—the instruction that NSA lives by still has my name on it. It's called USID-18.

Now what I'm setting up for you is a community whose job is surveillance, whose very existence is for surveillance, and that community was taught daily, regularly, signed an oath each year, retrained. And we focused on it in a way to carry out exactly the specifics of law. Let me contrast that with the FBI. FBI has a new mission. It's a new focus. And think of it in the previous time as arrest and convict criminals. Now it's to protect against terrorism, so it's a new culture adapting to a new set of authorities.

Now they were admitted by the Director of FBI and the Attorney General. Mistakes were made and they're cleaning that up. But it was done in a time when it was different in change, and that culture is evolving to do it.

Senator WYDEN. So you're saying that those who will handle the new FISA statute are more expert, and we'll want to inquire in secret session about that.

Now another section of the bill would grant immunity from liability to any person who provided support to the warrantless wiretapping program or similar activities. Would this immunity apply even to those who knowingly broke the law?

Director MCCONNELL. Of course not, Senator. It would never apply to anybody who knowingly broke the law.

Senator WYDEN. How is the bill going to distinguish between intentional lawbreakers from unintentional lawbreakers? One of the

things that I've been trying to sort out—and we've exchanged discussion about some of the classified materials—is, how are you going to make these distinctions? I mean, if we find out later that some government official did knowingly break the law in order to support the warrantless wiretapping program, could that then be used to grant them immunity? We need some way to make these distinctions.

Director MCCONNELL. Well, first of all, Senator, you're using the phrase "warrantless surveillance." Part of the objective in this proposal is to put all of the surveillance under appropriate authority, to include warrants where appropriate. Now if someone has violated the law, and it's a violation of the law, there could be no immunity.

Senator WYDEN. In January of this year, Attorney General Gonzales wrote to the Judiciary Committee and stated that any electronic surveillance that was being committed as part of the warrantless wiretapping program would "now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

Does this mean that the Federal Government is now obtaining warrants before listening to Americans' phone calls?

Director MCCONNELL. Sir, the way you're framing your question is if the intent was to listen to Americans' phone calls. That's totally incorrect.

Senator WYDEN. Well, simply——

Director MCCONNELL. The purpose is to listen to foreign phone calls. Foreign. Foreign intelligence. That's the purpose of the whole—think of the name of the Act—Foreign Intelligence Surveillance Act—not domestic, not U.S.

Senator WYDEN. But is the Federal Government getting warrants?

Director MCCONNELL. For?

Senator WYDEN. Before it's listening to a call that involves Americans?

Director MCCONNELL. If there is a U.S. person, meaning foreigner in the United States, a warrant is required, yes.

Senator WYDEN. The government is now, then, completely complying with the warrant requirement?

Director MCCONNELL. That is correct.

Senator WYDEN. OK.

Thank you, Mr. Chairman.

Chairman ROCKEFELLER. Thank you, Senator Wyden.

And we now go to Senator Feingold.

Senator FEINGOLD. Thank you very much, Mr. Chairman, for holding this hearing. And I have a longer statement I'd like to place in the record. And I'd ask the Chairman if I could do that.

Chairman ROCKEFELLER. Without objection.

[The prepared statement of Senator Feingold follows:]

PREPARED STATEMENT OF HON. RUSSELL D. FEINGOLD, A U.S. SENATOR FROM WISCONSIN

While I welcome this Committee's efforts to conduct oversight of the FISA process, I am extremely disappointed in the draft legislation the Administration has delivered to Congress. When the Administration finally chose to put the NSA's illegal warrantless wiretapping program under the Foreign Intelligence Surveillance Court process, I hoped we might have an opportunity to work together to determine if the

FISA statute needs to be updated to address any legitimate concerns about changes in technology.

Instead, the Administration has sent to Congress legislation that, while billed as FISA "modernization," is not only overbroad, but contains provisions having nothing to do with modernization of FISA. Those include full immunity to any entity that provided information to the government in the past six years as part of any "classified communications intelligence activity" which the Attorney General says is related to counterterrorism, and mandatory transfer to the secret FISA court of legal challenges to any "classified communications intelligence activity."

The Administration also continues to fail to cooperate with congressional oversight regarding past and current warrantless wiretapping activities. We must get answers to basic questions about these activities before we can seriously consider any significant changes to the statute.

Senator FEINGOLD. I thank the witnesses for testifying today.

Can each of you assure the American people that there is not—and this relates to the subject Senator Wyden was just discussing—that there is not and will not be any more surveillance in which the FISA process is side-stepped based on arguments that the President has independent authority under Article II or the authorization of the use of military force?

Director MCCONNELL. Sir, the President's authority under Article II is in the Constitution. So if the President chose to exercise Article II authority, that would be the President's call.

What we're attempting to do here with this legislation is to put the process under appropriate law so that it's conducted appropriately to do two things—protect privacy of Americans on one hand, and conduct foreign surveillance on the other.

Senator FEINGOLD. My understanding of your answer to Senator Wyden's last question was that there is no such activity going on at this point. In other words, whatever is happening is being done within the context of the FISA statute.

Director MCCONNELL. That's correct.

Senator FEINGOLD. Are there any plans to do any surveillance independent of the FISA statute relating to this subject?

Director MCCONNELL. None that we are formulating or thinking about currently.

But I'd just highlight, Article II is Article II, so in a different circumstance, I can't speak for the President what he might decide.

Senator FEINGOLD. Well, Mr. Director, Article II is Article II, and that's all it is.

In the past you have spoken eloquently about the need for openness with the American people about the laws that govern intelligence activity. Just last summer, you spoke about what you saw as the role of the United States stating that "Because of who we are and where we came from and how we live by law," it was necessary to regain "the moral high ground."

Can you understand why the American people might question the value of new statutory authorities when you can't reassure them that you consider current law to be binding? And here, of course, you sound like you're disagreeing with my fundamental assumption, which is that Article II does not allow an independent program outside of the FISA statute, as long as the FISA statute continues to read as it does now that it is the exclusive authority for this kind of activity.

Director MCCONNELL. Sir, I made those statements because I believe those statements with regard to moral high ground, and so on. I live by them.

And what I'm attempting to do today is to explain what it is that is necessary for us to accomplish to be able to conduct the appropriate surveillance to protect the American people, consistent with the law.

Senator FEINGOLD. Let me ask the other two gentlemen.

General Alexander, on this point with regard to Article II, I've been told that there are no plans to take warrantless wiretapping in this context, but I don't feel reassured that that couldn't reemerge.

General ALEXANDER. Well, I agree with the way Director McConnell laid it out.

I would also point out two things, sir. The program is completely auditable and transparent to you so that you and the others—and Senator Rockefeller, I was remiss in not saying to you and Senator Bond thank you for statements about NSA. They are truly appreciated.

Sir, that program is auditable and transparent to you so that you as the oversight can see what we're doing. We need that transparency and we are collectively moving forward to ensure you get that. And I think that's the right thing for the country.

But we can't change the Constitution. We're doing right now everything that Director McConnell said is exactly correct for us to.

Senator FEINGOLD. Well, here's the problem. If we're going to pass this statute, whether it's a good idea or a bad idea, it sounds like it won't be the only basis on which the Administration thinks it can operate. So in other words, if they don't like what we come up with, they can just go back to Article II. That obviously troubles me.

Mr. Wainstein?

Mr. WAINSTEIN. Well, Senator, as the other witnesses have pointed out, the Article II authority exists independent of this legislation and independent of the FISA statute. But to answer your question, the surveillance that was conducted, as the Attorney General announced, that was conducted pursuant to the President's terrorist surveillance program, is now under FISA Court order.

Senator FEINGOLD. Another topic. It would be highly irresponsible to legislate without an understanding of how the FISA Court has interpreted the existing statute. Mr. Wainstein, will the Department of Justice immediately provide the Committee with all legal interpretations of the FISA statute by the FISA Court along with the accompanying pleadings?

Mr. WAINSTEIN. I'm sorry, Senator; all FISA Court interpretations of the statute?

Senator FEINGOLD. All legal interpretations of the FISA statute by the FISA Court, along with the accompanying pleadings.

Mr. WAINSTEIN. In relation to all FISA Court orders ever——

Senator FEINGOLD. In relation to relevant orders to this statutory activity.

Mr. WAINSTEIN. Well, I'll take that request back, Senator. That's the first time I've heard that particular request, but I'll take it back.

Senator FEINGOLD. Well, I'm pleased to hear that, because I don't see how the Congress can begin to amend the FISA statute if it doesn't have a complete understanding of how the statute has been interpreted and how it's being currently used. I don't know how you legislate that way.

Mr. WAINSTEIN. Well, I understand, but obviously, every time they issue an order, that can be an interpretation of how the FISA statute is—interpretation of the FISA statute. And as you know from the numbers that we issue, we have a couple thousand FISAs a year. So that would be quite a few documents.

Senator FEINGOLD. This is an important matter. If that's the number of items we need to look at, that's the number we will look at.

Thank you, Mr. Chairman.

Chairman ROCKEFELLER. Thank you, Senator Feingold.

Senator Nelson.

Senator NELSON. Mr. Chairman, most of my questions I'm going to save for the closed session, but I would like to ascertain the Administration's state of mind with regard to the current law. In the case where there is a foreign national in a foreign land calling into the United States, if you do not know the recipient's nationality and therefore it is possible it is a U.S. citizen, do you have to, in your interpretation of the current law, go and get a FISA order?

Director MCCONNELL. No, sir. If the target is in a foreign country and our objective is to collect against the foreign target, and they call into the United States, currently it would not require a FISA. And let me double-check that. I may be—I'm dated.

General ALEXANDER. If it's collected in the United States, it would require a FISA. If it were known that both ends are foreign, known a priori, which is hard to do in this case, you would not. If it was collected overseas, you would not.

Senator NELSON. Let's go back to, General, your second answer.

General ALEXANDER. If you know both ends—where the call is going to go to before he makes the call, then you know that both ends were foreign; if you knew that ahead of time, you would not need a warrant.

Senator NELSON. If you knew that.

General ALEXANDER. If you knew that.

Senator NELSON. If you did not know that the recipient of the call in the U.S. is foreign, then you would have to have a FISA order.

General ALEXANDER. If you collected it in the United States. If you collected it overseas, you would not.

Senator NELSON. Well, since in digital communications, if these things, little packets of information are going all over the globe, you might be collecting it outside the United States, you might be collecting it inside the United States.

General ALEXANDER. And Senator, that's our dilemma. In the time in 1978 when it was passed, almost everything in the United States was wire, and it was called electronic surveillance. Everything external in the United States was in the air, and it was called communications intelligence.

So what changed is now things in the United States are in the air, and things outside are on wire. That's the——

Senator NELSON. I understand that. But I got two different answers to the same question from you, Mr. Director, and from you, General.

General ALEXANDER. It depends on where the target is and where you collect it. That's why you heard different answers.

Senator NELSON. So if you're collecting the information in the United States——

General ALEXANDER. It requires a FISA.

Senator NELSON. OK. Under the current law, the President is allowed 72 hours in which he can go ahead and collect information and, after the fact, go back and get the FISA order.

Why was that suspended before in the collection of information?

Director MCCONNELL. Sir, I think that would best be answered in closed session to give you exactly the correct answer, and I think I can do that.

Senator NELSON. Well, then, you can acknowledge here that it was in fact suspended.

Chairman ROCKEFELLER. I would hope that that would be—we would leave this where it is.

Senator NELSON. All right. I'll just stop there.

Chairman ROCKEFELLER. Thank you, Senator Nelson.

Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

The Administration's proposal, Admiral, doesn't address the authority that the President and Attorney General have claimed in conducting electronic surveillance outside of FISA. While the FISA Court issued a ruling that authorized the surveillance ongoing under the so-called TSP, Terrorist Surveillance Program, the White House has never acknowledged that it needs court approval. In fact, the President, under this reasoning, could restart the TSP tomorrow without court supervision if he so desired.

Now, Senator Specter and I have introduced legislation which very clearly establishes that FISA is the exclusive authority for conducting intelligence in the United States.

Here's the question. Does the Administration still believe that it has the inherent authority to conduct electronic surveillance of the type done under the TSP without a warrant?

Director MCCONNELL. Ma'am, the effort to modernize would prevent an operational necessity to do it a different way. So let me—I'm trying to choose my words carefully.

Senator FEINSTEIN. Yes, but my question is very specific. Does the President still believe he has the inherent authority to wiretap outside of FISA? It's really a yes or no question.

Director MCCONNELL. No, ma'am, it's not a yes or no question. I'm sorry to differ with you. But if you're asking me if the President is abrogating his Article II responsibilities, the answer is no. What we're trying to frame is—there was an operational necessary for TSP that existed in a critical period in our history, and he chose to exercise that through his Article II responsibility.

We're now on the other side of that crisis, and we're attempting to put it consistent with law, so it's appropriately managed and subjected to the appropriate oversight.

Senator FEINSTEIN. Well, the way I read the bill, very specifically, the President reserves his authority to operate outside of

FISA. That's how I read this bill. I think that's the defining point of this bill.

Not only that, in Section 402, Section 102(a), notwithstanding any other law, the President, acting through the Attorney General, may authorize electronic surveillance without a court order under this title, to acquire foreign intelligence information for periods of up to 1 year. And then it goes on to say if the Attorney General does certain things I mean, clearly this carves out another space. That's the question.

Director MCCONNELL. That same situation existed in 1978, when the original FISA law was passed. What we're attempting to balance is emergency response to a threat to the Nation, consistent with our values and our laws.

So the way this operated for 30 years, almost 30 years—we operated day to day, and it was appropriately managed and appropriate oversight. We had a crisis. The President responded to the crisis, and we're now attempting to accommodate new threats that we didn't understand in 2002, to be able to respond to protect the Nation, to protect the Nation and its citizens today, consistent with the appropriate oversight.

Does that mean the President would not exercise Article II in a crisis? I don't think that's true. I think he would use his Title II responsibilities under Article II.

Mr. POWELL. And Senator, if I may add, Section 402 is not meant to carve out in any way or speak to what the scope of the President's power is. That is meant to speak to Title III and criminal warrants and making clear what the certification procedure was. I was a part of this working group for over a year and a half, and the decision was specifically taken not to speak to, one way or the other, the scope of the President's constitutional power under Article II or to address that in this proposal in any way, whether to expand it or contract it; it was simply meant to be silent on what the President's Article II powers are.

I would also note, in the idea that the President can sidestep FISA or use Article II authority to simply place the statute aside, that is not my understanding of the Department of Justice position or the President's position. When you look at the legal analysis that has been released by the Department of Justice on the Terrorist Surveillance Program, that speaks to a very limited set, speaking to al-Qa'ida and its affiliates, in which we are placed in a state of armed conflict with, and speaking to the authorization of the use of military force passed by this Congress.

It does not speak to any kind of broad Article II authority of the President to simply decide to set FISA aside in toto and conduct electronic surveillance in a broad manner, unconnected to things like the authorization for the use of military force or the state of armed conflict that we entered into with al-Qa'ida.

So I have not seen anything from the Department of Justice or the President that would suggest that he would simply set aside FISA or has the authority to simply conduct electronic surveillance under Article II essentially unconnected to events in the world.

Senator FEINSTEIN. I can see that my time is up. But there is nothing in this bill which reinforces the exclusive authority of

FISA? There is nothing in this bill that confines the President to work within FISA?

Mr. POWELL. This bill does nothing to change what FISA currently says, which is electronic surveillance shall be—FISA shall be the exclusive means for conducting electronic surveillance unless otherwise authorized by statute. This bill simply leaves that statement as is. It does not strike it, it does not change it. It leaves it unchanged.

Senator FEINSTEIN. My time is up, but this is a good issue to pursue.

Thank you, Mr. Chairman.

Chairman ROCKEFELLER. Thank you, Senator Feinstein.

Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman.

We'll talk more about this obviously in the closed session, but I wanted to make a couple of points. And before I do, Director, let me say that I'm going to be speaking rather generally. As between you and I, I believe you to be an honorable and trustworthy man. I think that you are here with a view to be professional; that is your motivation. You are not an ideologue or a partisan in your desire to help repair the intelligence function of the United States, and I applaud you for that.

But that said, you are still asking for substantial changes in your authority. And as an aside, I think the new technologies that have emerged do suggest some adjustment to FISA. It may be over- or under-inclusive in certain areas. But as we look through the lens of the past in terms of evaluating how much we can trust you with institutionally—you know, these are tough times.

As you said, the reason we have FISA in the first place is because of past abuses. We've just found out about the litany of national security letter abuses within the Department of Justice. The Attorney General has thoroughly and utterly lost my confidence, and at this stage any element of the FISA legislation that depends on the Attorney General will need some other backstop in order to have my confidence.

We are coming out of this Article II regime of the TSP Program of warrantless wiretapping, and to this day, we have never been provided the Presidential authorizations that cleared that program to go or the Attorney General-Department of Justice opinions that declared it to be lawful.

Now, if this program is truly concluded, the TSP program, and if this is the new day in which everything is truly going to be under FISA, I can't imagine for the life of me why those documents that pertain to a past and closed program should not be made available to the Committee and to us. And so, to me, it's very concerning as we take these next steps for you to be saying impliedly, "Trust us, we need this authority, we'll use it well," when we're coming off the record of the national security letters; we're coming off terrible damage done to the Department of Justice by this Attorney General; we're coming off a continuing stonewall from the White House on documents that I cannot for the life of me imagine merit confidentiality at this stage.

And in the context of all of that you got some up-hill sledding with me, and I want to work with you and I want to do this, but

it would be a big step in the right direction, in terms of building the trust. Mr. Powell, I heard you just talk about how important it was that to the extent we've been disclosed, these opinions, that there was not transparency. We've been talking a lot about transparency and all that kind of stuff.

Where's the transparency as to the Presidential authorizations for this closed program? Where is the transparency as to the Attorney General opinions as to this closed program? That's a pretty big "We're not going to tell you" in this new atmosphere of trust we're trying to build.

If you have a response, sir, you'd like to make to that, I'd be delighted to hear it. I know it was not framed as a question.

Director MCCONNELL. I do have a response. I think the appropriate processes were created as a result of abuses of the seventies. They were inappropriate. We've got oversight Committees in both the Senate and the House. We're subjected to the appropriate oversight, rigorous, as it should be. Laws were passed to govern our activities. Those were inspected. We have inspectors general, and the process has worked well.

I've made a recommendation based on just coming back to the Administration with what we should do with regard to disclosing additional information to this Committee, and that recommendation is being considered as we speak. Certainly it's easier for me to share that information with you and to have a dialogue about what is said, and how it worked, and did it work well, and should we change it.

But until I get working through the process, I don't have an answer for you yet. But oversight is the appropriate way to conduct our activities going forward, consistent with the law.

Senator WHITEHOUSE. It's wonderful to hear you say that.

Mr. WAINSTEIN. If I may, Senator—may I just respond to that very briefly, Mr. Chairman?

Senator WHITEHOUSE. Please.

Mr. WAINSTEIN. Senator, to the extent that you've voiced some concern about lack of confidence in the Department of Justice and our role in FISA——

Senator WHITEHOUSE. No. Just to be clear—lack of confidence in the Attorney General.

Mr. WAINSTEIN. Well, if I may just say that I'm the head of a brand-new division that's focused on national security matters, and a large part of our operation is making sure that we play within the lines. We got a lot of people dedicated to that, and I can tell you that our Deputy Attorney General and our Attorney General are very conscientious about handling all FISA matters; they get reported to regularly and handle their responsibilities to sign off on FISA packages very carefully and conscientiously.

And as far as the NSL matter goes, both the Director of the FBI and the Attorney General were quite concerned about that and have put in place a very strong set of measures to respond to it. So I think if you look at their response to that problem, which was a very serious problem, I would hope that that would give you some more confidence.

Senator WHITEHOUSE. Thanks.

Chairman ROCKEFELLER. Thank you, Senator Whitehouse.

Senator Snowe.

Senator SNOWE. Thank you, Mr. Chairman.

Director McConnell, obviously this is creating this delicate balance. And I know in your testimony you indicated, as we redefine the electronic surveillance and obviously amend the Foreign Intelligence Surveillance Act, that to provide the greater, you know, flexibility in terms of communication, that we don't upset the delicate balance with respect to privacy questions.

Last September, Kate Martin, the director of the Center for National Security Studies, testified before the Crime, Terrorism and Homeland Security Subcommittee of the House Judiciary Committee and indicated that this bill would radically amend the FISA Act and eliminate the basic framework of the statute and create such large loopholes in the current warrant requirement that judicial warrants for secret surveillance of Americans' conversations and e-mails would be the exception rather than the rule. How would you respond to such a characterization? And could you also explain to the Committee how exactly the framework has been preserved through this renewed version of FISA?

Director MCCONNELL. Well, first of all, I characterize the statements you just read as uninformed, because the way it was framed, it's as if we were targeting without any justification communications of U.S. citizens, which is not the case, simply not the case. If there is a reason to target any communications and it's inside the United States, it would require a FISA warrant in the current law and in the future law.

So the only thing we're doing with the bill, the proposal, is just to update it to make it technology neutral. All things regarding privacy stay the same.

Senator SNOWE. And so in your estimation, then, there aren't any provisions in this proposal that would create such large loopholes.

Director MCCONNELL. No.

Senator SNOWE. No deviation, other than to make it technology neutral.

Director MCCONNELL. Zero. None.

Senator SNOWE. I noted in your statement that you mentioned additional protections besides coming before the respective intelligence Committees and also to the leadership regarding the Privacy and Civil Liberties Oversight Board that was established by the legislation that created the department in 2004. Exactly what has that board accomplished to this date? As I understand, it was just constituted last year in terms of all the appointments being completed. So exactly what has this board done in the interim that would suggest that they will provide additional oversight?

Director MCCONNELL. I've only met them recently and engaged with them and we have a regular cycle for meeting and discussing their activities, but it is oversight of the process to look at activities, to see what's being conducted, and they have a responsibility to report on it to the President and to others of us. They work in my organization to carry out their duties, which is to ensure that all of our activities are consistent with civil liberties and the appropriate protection of privacy.

Mr. POWELL. They've just released their first report. It's a detailed report, talks about the numbers of programs that they have reviewed, including an in-depth review of what was formerly the terrorist surveillance program before being placed under FISA. I think you'll find that report informative about what their findings were about the program. They've done some in-depth reviews of various programs both inside and outside the intelligence community, including they've attended NSA's training that is provided to its operators, and that is a public report.

Vito, you've interacted with them more. They've spent a lot of time in different programs across this government, and that report lays it out, and it's up on the Web.

Mr. POTENZA. No, Senator, there's not much more to add to that. They did come out to NSA. As Mr. Powell said, they sat in on training, they reviewed specifically the Terrorist Surveillance Program. They came out at least twice and spent a considerable amount of time with us.

Senator SNOWE. And when were they fully constituted as a board?

Director MCCONNELL. We have the head of the board here in the audience somewhere. Let me—get him to—he was here. Still with us?

Senator, I'll get back to you on it. I don't know the exact time, but we'll provide it to you.

Senator SNOWE. And certainly would they be giving I think reasonable assurances to the American people that they will be overseeing and protecting their privacy——

Director MCCONNELL. That's their purpose.

Senator SNOWE [continuing]. Consistent with the law?

Director MCCONNELL. That is their purpose, and as just mentioned, the first report is posted on the Web site. I didn't know it was actually already on the Web site.

Senator SNOWE. Thank you.

Chairman ROCKEFELLER. Thank you, Senator Snowe.

Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman.

The FISA Court interpreted or issued some orders in January. These are the orders which were the subject of some discussion here today. Do we have copies of all those orders, the January orders of the FISA Court?

Mr. WAINSTEIN. Yes. And all members of the Committee I think have been briefed in on them or——

Senator LEVIN. But do we have copies of the orders?

Mr. WAINSTEIN. I believe you all have copies, yes.

Senator LEVIN. How many are there?

Mr. WAINSTEIN. How many copies?

Senator LEVIN. How many orders?

Mr. WAINSTEIN. I cannot get into how many orders there are.

Senator LEVIN. You can't get into the number?

Mr. WAINSTEIN. Not in open session.

Senator LEVIN. Into the number of orders?

Mr. WAINSTEIN. Yeah, not in open session, Senator.

Senator LEVIN. OK. Have those orders been followed?

Mr. WAINSTEIN. Yes, sir.

Senator LEVIN. And have you been able to carry out the new approach that those orders laid out so far?

Mr. WAINSTEIN. I'd prefer to, if we could, defer any questions about the operation of the orders to closed session.

Senator LEVIN. No, I'm not getting into the operations. I want to know, have you been able to implement those orders?

Mr. WAINSTEIN. We have followed the orders, yes, sir.

Senator LEVIN. Without any amendments to the statute?

Mr. WAINSTEIN. There have been no amendments to the statute since the orders were signed in January.

Senator LEVIN. And you've been able to follow the new orders without our amending the statute?

Mr. WAINSTEIN. We have——

General ALEXANDER. Sir, could I——

Senator LEVIN. Just kind of briefly, I mean let me ask the question a different way. Are the orders dependent upon our amending the statute?

General ALEXANDER. No, the current orders are not.

Senator LEVIN. OK.

General ALEXANDER. Nor are the current orders sufficient for us to do what you need us to do.

Senator LEVIN. I understand that. But in terms of the orders being implementable, they do not depend upon our amending the statute. Is that correct?

General ALEXANDER. That's correct. The current state that we're in does not require that.

Senator LEVIN. Good.

General ALEXANDER. But I would also say, that's not satisfactory to where you want us to be.

Director MCCONNELL. Senator, what you need to capture is, we were missing things that——

Senator LEVIN. I understand. I understand that we're not deterring the implementation of the orders.

Now back in January, there was an article that says that the Administration continues to maintain that it is free to operate without court approval. There seemed to be some question about that here today. Is that not the Administration's position?

Director MCCONNELL. That is not the Administration's position that I understand, sir.

Senator LEVIN. OK.

Back in January, on the 17th, the Attorney General wrote to Senators Leahy and Specter the following, that a judge of the Foreign Intelligence Surveillance Court issued orders authorizing the government to target for collection international communications into or out of the United States, where there is probable cause to believe that one of the communicants is a member or agent of al-Qa'ida or an associated terrorist organization. Has that remained the test for when you want to be able to target a communication where the target is in the United States, is that, there must be probable cause to believe that one of the communicants is a member or agent of al-Qa'ida or an associated terrorist organization?

Mr. POWELL. Senator, I think it would be best if we get into that in closed session.

Senator LEVIN. Well, is there any change in that? This to me is the key issue, the probable cause issue——

Mr. POWELL. Senator, you have copies of those orders that lay out very specifically what those tests are. What the Attorney General's letter did was speak to what the President had laid out in his December 17, 2005 radio address as the Terrorist Surveillance Program.

Senator LEVIN. I understand.

Mr. POWELL. And that is what that letter is addressed to, Senator.

Senator LEVIN. My question is, is there any change, that that is what you are limiting yourselves to, situations where, if the target is in the—if the eavesdropping takes place in the United States, that there must be probable cause to believe that one of the communicants is a member or agent of al-Qa'ida or an associated terrorist organization? Is there any change from that? This is what the Attorney General wrote us. Is there any change from that since January 17?

General ALEXANDER. Sir, we can't answer that in open session.

Senator LEVIN. Well, he wrote it in open session. It's an open letter.

Vice Chairman BOND. Mr. Chairman, I would suggest to the Chairman that this question we can explore fully in the closed session.

Senator LEVIN. Well——

Chairman ROCKEFELLER. I would leave that——

Senator LEVIN. This is a letter which was written publicly. If there's a change to this, we ought to know about that publicly.

Chairman ROCKEFELLER. If that represents a program, say so.

Director MCCONNELL. It presents a problem for us, sir.

Chairman ROCKEFELLER. It is not——

Director MCCONNELL. It presents a problem for us. The way it was framed and the way it was written at the time is absolutely correct. The way the Senator's framing his question, it pushes it over the edge for how we can respond to it, because there's been some additional information.

Senator LEVIN. Could the Attorney General write that letter today?

Director MCCONNELL. We can discuss it in closed session, sir.

Mr. POWELL. Senator, the point of the Attorney General's letter, as I understood it, was to address those things that the President had discussed that were being done under the Terrorist Surveillance Program. And what his letter addresses is to say that those things that the President had discussed under the program were now being done under orders of the FISA court. And today, as we sit here, the Attorney General's letter remains the same—that those things that the President had discussed continue to be done under the orders of the FISA court. So to that extent, there's no change to the Attorney General's letter.

General ALEXANDER. Sir, if I could, to just clarify this one step further, there are other things that the FISA court authorizes day in and day out that may be included in that order, that go beyond what the Attorney General has written there. Every day we have new FISA applications submitted.

What you were tying this to, Senator, was al-Qa'ida.

Senator LEVIN. Mr. Chairman, I think, if the Chair and Vice Chair are willing, I think we ought to ask the Attorney General then if this letter still stands.

In terms of the test which is being applied for these targeted communications, it's a very critical issue. The President of the United States made a representation to the people of the United States as to what these intercepts were limited to. And the question is, is that still true? And it's a very simple, direct question, and we ought to ask the Attorney General, since he wrote, made a representation in public; the President has made a representation in public. If that's no longer true, we ought to know it. If it is still true, we ought to know it. So I would ask the Chairman and Vice——

Chairman ROCKEFELLER. The Senator is correct, and that will happen and that will be discussed in the closed session.

Senator LEVIN. Thank you. My time is up. Thank you.

Chairman ROCKEFELLER. No, thank you, Senator Levin. After Vice Chairman Bond has asked his question, I'm yielding my time to the Senator from Florida, and I guess then to the Senator from Oregon, and then eventually I'll get to ask a question, too.

Senator Bond.

Vice Chairman BOND. Thank you, Mr. Chairman. I think maybe to clear up some of the confusion and some of the questions couldn't be answered, it's my understanding you're before us today asking for FISA updates to enable NSA to obtain under that statute vital intelligence that NSA is currently missing.

And secondly, when we talk about Article II and the power of the President under Article II, Presidents from George Washington to George Bush have intercepted communications to determine the plans and intentions of the enemy under the foreign intelligence surveillance authority in that. And prior to the TSP, as I understand it, the most recent example was when the Clinton Administration used Article II to authorize a warrantless physical search in the Aldrich Ames espionage investigation.

The Supreme Court in the Keith case in 1972 said that the warrant requirement of the Fourth Amendment applies to domestic security surveillance, but it specifically refused to address whether the rule applied with respect to activities of foreign powers or their agents. And then in the Truong case in 1980, the Fourth Circuit noted the constitutional responsibility of the President for the conduct of the foreign policy of the United States in times of war and peace in the context of warrantless electronic surveillance. And it did say that it limited the President's power with a primary purpose test and the requirement that the search be a foreign power, its agent or collaborator.

Finally, despite Congress' attempts to make FISA the exclusive means of conducting electronic surveillance for national security purposes, my recollection from law school is that the Constitution is the supreme law of the land. It is a law.

Congress cannot change that law in the Constitution without amending the Constitution. And the Foreign Intelligence Court of Review, in In re Sealed Case, in 2002, Judge Silverman wrote, "We take for granted that the President does have the authority"—

that's the authority to issue warrantless surveillance orders—"and assuming that is so, FISA could not encroach on the President's constitutional power. We should remember that Congress has absolutely no power or authority or means of intercepting communications of foreign enemies. So even at his lowest ebb, the President still exercises sufficient significant constitutional authority to engage in warrantless surveillance of our enemies".

And I know that there are two admitted lawyers on the panel. Are you a lawyer also? Three. Is that right? Is that correct? Mr. Powell, Mr. Wainstein, Mr. Potenza. Thank you.

Chairman ROCKEFELLER. Just for the record, they nodded "yes." [Laughter.]

Vice Chairman BOND. But we didn't want to disclose all the lawyers on there. I have that problem myself.

I wanted to ask, since we're asking kind of unrelated questions, Mr. Wainstein, the 9/11 Commission and this Committee tried to get a look at all the intelligence and the policy decisions leading up to 9/11. And I'm beginning to hear that we did not and maybe the 9/11 Commission did not get all the information.

For example, in the case of Mr. Sandy Berger, he admitted removing five copies of the same classified document from the National Archives; destroyed three copies. We know that he was there on two other occasions; we don't know whether he removed other original documents. He removed classified notes without authorization. What we don't know is what was actually in the PDBs that were stuffed in his BVDs. In his plea agreement, he agreed to take a polygraph at the request of the government, and for some reason, the Department of Justice has not gotten around to polygraphing him to ascertain what was in the documents and why he removed them.

Are you going to try to find out that information, and when can you let us know, Mr. Wainstein?

Mr. WAINSTEIN. Senator Bond, I know that that is an area of inquiry from other Members of Congress, and there's been a good bit of traffic back and forth on that particular issue. I have to admit that right now I'm not up on exactly where that is. So if it's OK with you, I will submit a response in writing.

Vice Chairman BOND. We'd like to find out.

Thank you, Mr. Chairman.

Mr. WAINSTEIN. Thank you, sir.

Chairman ROCKEFELLER. Thank you, Mr. Vice Chairman.

And now Senator Nelson, to be followed by Senator Wyden, to be followed by myself.

Senator NELSON. Thank you, Mr. Chairman.

I want to go back to the line of questioning before. You already said that under current law, if there is someone who is deemed to be of interest outside of the United States that's calling in, even though we may not know that the person in the United States is a U.S. citizen, that under current law that would require a FISA order?

Director MCCONNELL. It depends on where the intercept takes place.

Senator NELSON. OK. And so if the intercept takes place in the United States——

Director MCCONNELL. It requires an order.

Senator NELSON. OK. Now——

Mr. POTENZA. Senator, if I may, I would just add to that. If it's on a wire in the United States, it requires a FISA order.

Senator NELSON. So if it's a cell phone, it doesn't require—if it——

Mr. POTENZA. A separate section of FISA would cover that. But the particular situation you were talking about is the wire section.

Director MCCONNELL. In 1978, they separated it between "wire" and "wireless." And so if a wireless call was made from overseas into the United States via satellite, it would be available for collection.

Senator NELSON. Right. Is it the case under current law where all parties to a communication are reasonably believed to be in the United States, that the government would need to go to a FISA court to obtain an order authorizing the collection?

Director MCCONNELL. Yes, sir, that's correct.

Senator NELSON. Under your new proposal, is that the case?

Director MCCONNELL. That's correct. Yes, sir, it is correct.

Senator NELSON. The proposed definition of electronic surveillance depends on whether a person is reasonably believed to be in the United States. What kind, Mr. Wainstein, of guidance would the Justice Department give when someone is reasonably believed to be in the United States?

Mr. WAINSTEIN. Sir, I can't give you specific indicia that we would use. We might be able to elaborate more in closed session as to what NSA, what kind of indicia NSA actually uses right now. But it's exactly that. In telecommunications, it's not always a certainty these days exactly where a communicant is. So we have to use the information we have to make a reasonable determination as to where that person is.

Director MCCONNELL. But if we know, if the collector knows you're in the United States, it requires FISA.

Senator NELSON. OK. Now, if you know that two people are in the United States, and you are collecting that information in the United States, normally that would require a FISA order.

Director MCCONNELL. Yes, sir.

Senator NELSON. Does that include if you know one of those people on the communication in the United States is a member of al-Qa'ida?

Director MCCONNELL. Yes, sir.

Senator NELSON. It still does. OK.

Mr. Chairman, I want to turn back to the question that I asked before. And you stop me, as you did before, if you don't want me to proceed. But it was openly discussed in all of the public media that the 72-hour rule under current law was not obeyed with regard to the intercepts that have occurred.

And my question was—well, I first asked why, but then I asked did it, in the Administration. I would like an Administration witness to answer if what we read in the New York Times and the Washington Post and the L.A. Times and the Miami Herald about the 72-hour requirement not being complied with, is that true, that it wasn't complied with, the law, the current law?

Mr. POWELL. Senator, when you're referring to the 72-hour rule, I think you're referring to the emergency authorization provisions by which the Attorney General, if all of the statutory requirements are met to the Attorney General's satisfaction, he may authorize surveillance to begin and then has 72 hours after that to go to the FISA Court. If that is what you're referring to, Senator——

Senator NELSON. Well, that's what I stated in my previous question when the Chairman stopped me.

Mr. POWELL. Senator, what the President discussed in his radio address, I believe, of December 17, talking about one-end communications involving al-Qa'ida or an affiliate, those were done under the President's authorization and the President's authority, were not done pursuant to FISA or Attorney General emergency authorizations by which after 72 hours you would go to to the FISA Court. To that extent the emergency authorization provision of FISA was not a part of that terrorist surveillance program.

Senator NELSON. Well, here's the trick, and I'll conclude. The trick is we want to go after the bad guys, we want to get the information that we need, but we're a nation of laws and we want to prevent the buildup of a dictator who takes the law into his own hands, saying, "I don't like that."

So now we have to find the balance. And that's what we need to craft, because there is legitimate disagreement of opinion on the interpretation that the President broke the law the last time. Senator Bond would say, no, he didn't, because he had an Article II constitutional right to do that.

Well, this is what the American people are scared about, that their civil rights and civil liberties are going to be invaded upon because somebody determines, outside of what the law says in black and white, that they know better than what it says. And so we've got to craft a new law that will clearly make that understandable.

Thank you, Mr. Chairman.

Chairman ROCKEFELLER. Thank you, Senator Nelson. Senator Wyden, I'll get you in just a second.

The Chairman would say very strongly here at this point that this in fact a creative process, and that those who watch or listen or whatever—it's OK that we do this. What it does say is that what we were discussing is incredibly important for the national security, as is what we're talking about, incredibly important for individual liberties. It is wholly understandable, and it is wholly predictable, in this Senator's view, that there would be areas where we would come to kind of a DMZ zone, unhostile, and where one side or another would get nervous.

It is the judgment of this Chairman that in a situation like that, when you're dealing with people who run the intelligence, that you respect their worry, because you do not have to worry about the fact that the information will come out. Because we do have a closed hearing, and all members will be at that closed hearing. And they will hear the answers to the questions that have been asked.

So that—I don't have a hesitation if I feel, and the Vice Chairman on his part has that same right, if there's a feeling that we're getting too close to the line, let's not worry too much about that. We have not crossed that line. The Senator from Florida extended

my cutoff, as he said, a little bit further. There was not particular objection on your part, and so the situation has been resolved.

But I just wanted to make that clear. When we're in open session, this is the only Committee on this side of the Capitol Building which runs into conflicts of this sort, potential conflicts of this sort. And we darn well better be very, very careful in the way that we resolve them and err, from my point of view, with a the sense of caution.

Because if we're going to craft something—and Senator Bond and I have been talking about this a little bit during the hearing—if we're going to craft something which can get bipartisan support, which is what we need, we need to have not only the trust but also the integrity of discourse.

Words can do great damage. They can do great good. Silence can do great damage. Silence can do great good.

So I consider all of this useful, and I now turn to Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. I happen to agree that both you and Senator Bond have made valid points on this. And what concerns me is, too much of this is still simply too murky.

And I think, with your leave, Admiral McConnell, let me just kind of wade through a couple of the other sections that still concern me.

Section 409 on physical searches creates a new reason to hold Americans' personal information obtained in a physical search, even when a warrant is denied. And I want to kind of walk you through kind of existing law and then the change and get your reaction.

Current law allows the Attorney General to authorize a secret emergency search of an American's home, provided that the government gets a warrant within three days of the search. If the warrant is denied, then information gathered in the search may not be used unless it indicates a threat of death or harm to any person. I think virtually nobody would consider that out of bounds. That's a sensible standard in current law.

But the bill would permit the government to retain information gathered in the secret search of an American's home, even if the warrant is later denied, if the government believes there is something called significant foreign intelligence information. How is that definition arrived at? What is the process for that additional rationale for keeping information on hand after a warrant is denied?

Director MCCONNELL. Sir, I'll turn to the lawyers for a more official definition of that, but the way I would interpret it as an operator is, it would be threat information, something of a planning nature that had intelligence value, that would allow us to prevent some horrendous act. So it would be something in the context of threat.

Senator WYDEN. What amounts to an imminent act.

Director MCCONNELL. Imminent or a plan for, you know blowing a bridge or something of that nature.

Senator WYDEN. I was searching for the word "imminent," and I appreciate it.

The lawyers, I'll move on, unless you all want to add to it. But I was searching for the word "imminent " Do you all want to that? Because I want to ask one other question.

Mr. POWELL. Well, I just want to make it clear, Senator, that you did represent the proposal correctly, that the words "significant foreign intelligence information" would go broader, to just something that is imminent or a terrorist event. So the proposal is broader there, to allow the government to retain and act upon valuable foreign intelligence information that's collected unintentionally, rather than being required to destroy it if it doesn't fall in the current exception. But you represented the proposal correctly, Senator.

Senator WYDEN. All right. Let me ask a question now about 408, and this goes back to the point that I asked you, Admiral, earlier about that a section of the bill grants immunity from liability to any person who provided support to the warrantless wiretapping program or similar activities. I asked whether the immunity would apply even to persons who knowingly broke the law, and I asked what is in Section 408 that distinguishes intentional lawbreakers from unintentional ones. And I still can't find it after we've gone back and reviewed it.

Can you and the lawyers point to something there—it's at page 35, Section 408—that allows me to figure out how we make that distinction?

Mr. POWELL. Right, Senator. 408, the liability defense, what it would do is say that the Attorney General or a designee of the Attorney General would have to certify that the activity would have been intended to protect the United States from a terrorist attack.

The Attorney General would actually have to enter a certification for anybody to be entitled to this defense. I don't believe the Attorney General or the designee would issue such a certification for somebody who was acting in the manner that you've described.

Senator WYDEN. So that essentially is how you would define the last seven or eight lines of page 35, is that the Attorney General would have to make that certification.

Mr. POWELL. That's correct, Senator. It's not a defense that somebody could just put forth without having the Attorney General involved in a certification process.

Senator WYDEN. Gentlemen, I think you've gotten the sense from the Committee that one of the reasons that the bar is high now is that the American people have been told repeatedly—both with respect to the national security letters that I touched on earlier, the PATRIOT Act and other instances—we've been told in language similar to that used today that steps were being taken to assure that we're striking the right balance between fighting terrorism and protecting people's privacy. And that is why we're asking these questions. That's why we're going to spend time wading through this text.

Admiral, you've heard me say both publicly and privately, you've been reaching out to many of us on the Committee to go through these specific sections. You've got a lot of reaching out to do, based on what I've heard this afternoon and, I think, what I've heard colleagues say today.

But we're interested in working with you on a bipartisan basis, and I look forward to it.

Thank you, Mr. Chairman.

Director MCCONNELL. Thank you, Senator.

Chairman ROCKEFELLER. Thank you, Senator Wyden.

I'll conclude with three questions, unless the Vice Chairman has further questions.

This is listed as all witnesses. I'd like a little minimization there. A criticism of the Administration's bill is that while the reasons given for the bill are focused on the need to respond to the threat of international terrorism, the Administration's bill would authorize warrantless surveillance of all international calls for any foreign intelligence purpose.

How would you respond to a suggestion that a more narrow approach be considered that would specifically address communications associated with terrorism, as opposed to the blanket foreign intelligence purposes in the Administration's proposal?

Director MCCONNELL. Sir, if it's inside the United States, regardless, it would require a warrant, as it does today. So if the foreign intelligence originated in a foreign location and it has to do with intelligence of interest to the United States, such as weapons of mass destruction shipment or something to do with a nation state not necessarily associated with terrorism, that would still be a legitimate foreign intelligence collection target. So something inside the United States requires a warrant. External to the United States, what we're arguing is it should not require a warrant, as we have done surveillance for 50 years.

Chairman ROCKEFELLER. Thank you.

Mr. Wainstein, the Administration's bill would expand the power of the Attorney General to order the assistance of private parties without first obtaining a judicial FISA warrant that is based on the probable cause requirements in the present law. A limited form of judicial review would be available under the Administration's bill after those orders are issued.

Why is this change necessary? Has the FISA Court's review of requested warrants been a problem in the past?

Mr. WAINSTEIN. Mr. Chairman, I believe what you're referring to is Section 102, large A. And what that does is it says that for those communication interceptions that no longer fall under FISA, with the redefinition of electronic surveillance, that there's a mechanism in place for the Attorney General to get a directive that directs a communications company to assist in that surveillance, because there's no longer a FISA Court order that can be served on that company. So this way the Attorney General has a mechanism to get a directive to ask a company to provide the assistance that's necessary.

If that company disagrees with that and wants to challenge that order, this proposal also sets up a mechanism by which that company can challenge that order to the FISA Court. So there is judicial review of any compulsion of a communications provider to provide communications assistance to the government.

Chairman ROCKEFELLER. And there are precedents in American law for such?

Mr. WAINSTEIN. Yes, in a variety of different ways, both on the criminal side and on the national security side, yes, sir.

Chairman ROCKEFELLER. OK. My final question is also to you, sir. The Administration argues that if these FISA amendments were enacted, there could be greater attention paid to the privacy protections of persons in the United States. Among these amendments, however, are provisions that would presumably limit the amount of information being provided to the Foreign Intelligence Surveillance Court.

The proposed amendments, for example—and here we get back to what has already been discussed—provide for the use of "summary description," rather than "detailed description" in FISA applications when it comes to "the type of communications or activities to be subjected to surveillance."

Is the Department of Justice seeking to limit the information a judge of the FISA Court has available upon which to base a decision and issue and order for electronic surveillance? And if that be the case, why?

Mr. WAINSTEIN. Mr. Chairman, I appreciate the question. And those specific proposed revisions essentially say that instead of providing very detailed explication of those points that you just cited, the government can provide summary information. And that's a recognition of the fact that right now the typical FISA Court package that goes to the court is, you know, 50-60 pages, something in that range. It's a huge document. And a lot of that information is or more or less irrelevant to the ultimate determination of probable cause. It needs to be there in summary fashion, but not in detailed fashion.

So that's all those streamlining provisions are doing. They're not in any way denying the FISA court the critical information they need to make the findings that are required under the statute.

And in terms of our statements that this overall bill will protect the privacy rights of Americans, frankly, it's a very practical point, which is that right now we spend a lot of time—in the Department of Justice, NSA and the FISA Court—focusing on FISA packages that really don't relate to the core privacy interests of Americans. They relate to these FISA intercepts, which really weren't intended to be covered by FISA. If those are taken out of FISA so that we're focusing back on privacy interests of Americans, then all that personnel, all that attention will be focused where it should be, on Americans and on Fourth Amendment interests here in the United States.

Mr. POWELL. And, Senator, if I could add—because there's a lot of attention to Department of Justice and attorney resources—a critical piece on this is that these applications in many cases resemble finished intelligence products. The burden is on the analysts and the operators, so it's not a matter of more resources for the Department of Justice, that we could bring lawyers on board and bring them in, and they would somehow magically understand the cases and be able to produce what are essentially finished intelligence products, in some cases, for the court; we think that where we've gotten to in the place with the statute has gone beyond what anybody ever intended.

The burden of that falls on the analysts and operators of the intelligence community, not the lawyers, Senator. We ask the questions and we write them down and we put the packages together,

but it's a huge burden to put this type of product together with people who are very limited, whose time is very limited, and they need to spend time sitting with me and Ken's staff to produce these products. So it's not just a question of Department of Justice resources. I think that would be a solvable problem. The issue really becomes kind of the limited analysts and operators that are working these cases in real time.

Chairman ROCKEFELLER. If what you suggest is—and I'm actually growing a little weary of this term, the "burden"—the "burden"—there are a lot of burdens in government, there's a lot of paperwork in government. Go work for CMS someday and you'll get a real lesson in burden. Is the burden that you're referring to too much paperwork, don't have time, can't respond in time? Is that what the courts are saying or is that what you are saying?

Mr. POWELL. Yeah, I think the issue is not the—it's the issue of—it's not the burden to focus on what the balance was struck in 1978, to focus on U.S. persons in the United States. What we have done is taken a framework that was designed to prevent domestic abuses that threatened our democratic institutions. That was meant to protect against that and the abuses that happened—and we can talk about those—and we've just simply, because of the way technology has developed, transferred that framework to people who were never intended to be a part of that, and where that danger, frankly, does not exist.

So we've taken a framework designed to prevent domestic abuses, and, simply because of technological changes, transferred this to foreign entities, and I don't think I have not heard any reasonable argument that those activities directed at foreign entities not in the United States somehow present the same threats that we were concerned about domestically. So we've shifted the entire framework simply because of technology. We've shifted a good portion of that framework to a situation that is completely different, and we put back in place that original balance that we believe was struck in 1978, Senator.

Chairman ROCKEFELLER. Well, it occurs to me—and these are my closing remarks—is that changing technology is a part of every aspect of all of our lives.

And so we all live with it every day in many ways; some catch up, some don't. You have to be ahead of the curve, and you have to be able to respond very rapidly.

I think it's going to be very important—and Senator Bond and I have discussed this during this hearing and before—that we come out with a solution that works on this. I think it would be very damaging if we did not. I think it would be very damaging if we came out with a solution which went along purely partisan lines and was based upon arguments from one end to another.

Having said that, I'm not sure it's going to be easy, and that's why the intelligence, the orders that we have not received chafe at the Vice Chairman and myself. When you're not completed, when you're not given complete information on something which is so fundamental and where the line between privacy and security has to be so exact, then there can be a real sense of frustration, if only because you fear you're not acting on complete information. It has nothing to do with our trusting of all of you. It has to do with the

process which is meant to inform the intelligence Committees in the Senate and the House of what the legal underpinning is.

So I would repeat my request, particularly to the Director of National Intelligence, that this is a matter not just of letters that have been written and requests which have been made, but a matter of the really important fundamental ability of us to work together as a Committee to produce a good product. I want a product that works for America. Senator Bond wants a product that works for America. There are going to have to be some adjustments made, as there inevitably will, or else we just go on in some kind of a food fight which is no good for anybody at all.

So I would ask that cooperation, and I would renew my request for the information that I asked for in my opening statement.

Vice Chairman BOND. Mr. Chairman, I join with you in asking for the legal justifications. Now I recognize in some attorney-client relationships the opinions reflect the negative side rather than the positive side, and I don't know what would be in that information.

But suffice it to say that we need specifically, succinctly the legal justifications and a copy of the kind of orders that went out, so we can see what went on.

On the other hand, when we're on another issue, when we're talking about FISA applications, Mr. Powell, how many FISA applications are made a year?

Mr. POWELL. I think Mr. Wainstein will have the numbers. I have them in my bag, Senator. They're in the report that is publicly filed each year.

Mr. WAINSTEIN. I think the most recent number was 2,183 for 2006.

Vice Chairman BOND. 2,183, and they average about 50 pages?

Mr. WAINSTEIN. About that, yes, sir.

Vice Chairman BOND. So 50 pages times that. My math is a little slow. But each year that would be over roughly 110,000 pages. And each year we go back would be another 100,000. I think we ought to—there was a question about having all FISA orders.

I think we need to come to a reasonable agreement on maybe—I don't know where we would put 100,000 pages of orders. And I think that we need to look at that and find a way to issue a request that can be responded to and that we can handle. But I do believe very strongly that clear, succinct legal justification should be shared with us when we're in the closed hearings.

And we got into the fringe areas of a lot of things that the Chairman and I know why it could not be answered. And while it may appear that there was a lack of forthcoming by our witnesses, we know full well what it is that prevents your answering it. And we will look forward to getting all those answers.

And I think it will become clear to all of us, the Chairman and the Vice Chairman and the Members, when you can lay out the specific reasons that we danced around today as to why and what and where FISA needs to be changed. And I thank you, Mr. Chairman, and I thank our witnesses.

Chairman ROCKEFELLER. And the hearing is adjourned.

[Whereupon, at 4:50 p.m., the Committee adjourned.]

Statement of Kevin S. Bankston
Staff Attorney
Electronic Frontier Foundation

before the
Senate Select Committee on Intelligence

on
FISA Modernization

May 1, 2007

Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee, the Electronic Frontier Foundation (EFF) is pleased to have this opportunity to provide its statement on the Administration's current proposal to "modernize" the Foreign Intelligence Surveillance Act (FISA).[1]

EFF is a non-profit, member-supported public interest organization dedicated to protecting privacy and free speech in the digital age. As part of that mission, EFF is representing current and former residential customers of AT&T in a civil action against that company for its alleged cooperation in the National Security Agency's warrantless dragnet surveillance of its customers' telephone calls and Internet communications.[2] Just as Congress' laws prohibiting warrantless electronic surveillance bind the government, so too do they bind those telecommunications carriers that are entrusted with transmitting Americans' private communications. As Congress recognized when it provided civil causes of action against communications providers that violate that trust, the ability to maintain such lawsuits is a key check against illegal collaborations between the Executive and those that control access to our national telecommunications infrastructure.

The amendments to FISA currently proposed by the Administration threaten to deprive our plaintiffs of their day in court, and to deprive all Americans of their right to communicate privately. That proposal, far from "modernizing" the law, would gut the long-standing checks and balances that Congress established to rein in the Executive's ability to spy on Americans. It would shield surveillance conducted in the name of national security from meaningful judicial scrutiny, and unjustifiably provide blanket immunity for illegal surveillance conducted since September 11, 2001—surveillance that

---

[1] FISA Modernization Provisions of the Proposed Fiscal Year 2008 Intelligence Authorization, Title IV, *available at* http://www.fas.org/irp/news/2007/04/fisa-proposal.pdf (hereinafter "Administration Proposal").
[2] *Hepting v. AT&T*, 439 F.Supp.2d 974 (N.D. Cal. 2006) (on appeal to the Ninth Circuit).

454 Shotwell Street, San Francisco, CA 94110 USA
+1 415 436 9333 (v) +1 415 436 9993 (f) www.eff.org

Congress has not yet even investigated, and which appears to go far beyond the narrow "Terrorist Surveillance Program" admitted to by the President.[3]

Unfortunately, this Administration has squandered the people's trust over the past five years, flagrantly ignoring FISA's requirements by wiretapping Americans without warrants and routinely abusing its authority under the USA PATRIOT Act to obtain Americans' private records.[4] It can no longer be given the benefit of the doubt by Congress in these matters. When a large margin of Americans believe that the President has failed to properly balance the preservation of civil liberties against national security concerns,[5] what is most needed is vigorous investigation and oversight by Congress and the Courts—not a statutory blank check granting the Executive even greater surveillance authority, nor a pardon for government agents and telecommunications companies that have violated the law in the past. The Administration and the telephone companies must understand that they cannot ignore the statutes passed by Congress and then simply demand amnesty when caught in the act.

Other commentators have already explained at length how passage of the Administration's proposal as a whole would dangerously and unjustifiably expand the Executive's surveillance powers.[6] Therefore, this statement will focus on those provisions that would most directly impact pending lawsuits against the government and telecommunications carriers for their illegal collaboration in the surveillance of Americans' private communications. In particular, this statement will address:

- Section 408, "Liability Defense," which would unjustifiably grant broad immunity to those who have illegally spied on American citizens;

---

[3] *See, e.g.*, Eric Lichtblau and James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, The New York Times (December 24, 2005), at A1; Leslie Cauley and John Diamond, *Telecoms Let NSA Spy On Calls*, USA Today (February 6, 2006), at A1.

[4] *See* U.S. Department of Justice Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (March 2007), *available at* http://www.usdoj.gov/oig/special/s0703b/final.pdf.

[5] *See* Shaun Waterman, *Analysis: Poll Shows Security Imbalance*, United Press International (April 26, 2007), *available at* http://www.upi.com/Zogby/UPI_Polls/2007/04/26/analysis_poll_shows_security_imbalance/.

[6] *See, e.g.*, Letter of the American Civil Liberties Union to Chairman Rockefeller and Vice Chairman Bond (April 16, 2007), *available at* http://www.aclu.org/images/general/asset_upload_file827_29385.pdf; Center for Democracy & Technology, *"Modernization" of the Foreign Intelligence Surveillance Act (FISA): Administration Proposes Broad, Warrantless Surveillance of Citizens* (last updated April 18, 2007), *available at* www.cdt.org/security/20070418fisaanalysis.pdf; and Center for National Security Studies, *Fact v. Fiction: The Justice Department's "New" Re-Write of FISA* (April 18, 2007), *available at* http://www.cnss.org/FinalCNSS%20FISA%20Memo%204.19.07.pdf.

- Section 406, "Use of Information," which threatens to create a back door immunity by allowing the Administration to argue that its common law privilege against the disclosure of state secrets overcomes the carefully balanced statutory procedures that Congress established to facilitate litigation over the legality of electronic surveillance; and
- Section 411, "Mandatory Transfer for Review," which would further strengthen the Executive's hand by allowing it to transfer all cases concerning its illegal surveillance to the court most likely to rule in its favor.

Taken together, these provisions represent a concerted attack on the rights of Americans to seek redress when subjected to illegal surveillance, and are an obvious attempt to shield the Administration and its collaborators against judicial inquiry into their illegal surveillance activities since 9/11.

I. Section 408: Blanket Immunity for Illegal Surveillance

The Administration has repeatedly assured Congress and the public that its warrantless surveillance of Americans is fully consistent with the law.[7] Those claims ring hollow, however, when read in conjunction with Section 408 of its proposal. With Section 408, the Administration seeks to provide blanket immunity against liability to any person who has assisted in any government surveillance activity that the Attorney General or his designee claims was undertaken in the name of anti-terrorism. The Administration's bid for such immunity essentially concedes the weakness of its legal arguments in support of warrantless surveillance, arguments that it clearly hopes to insulate from judicial scrutiny.

Specifically, the breathtakingly broad terms of Section 408 provide that:

> Notwithstanding any other law, and in addition to the immunities, privileges, and defenses provided by any other source of law, no action shall lie or be maintained in any court, and no penalty, sanction, or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities, or any other form of assistance, during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act, in connection with any alleged classified communications intelligence activity that the Attorney General or a designee of the Attorney General certifies, in a manner consistent with the protection of State secrets, is, was, would be, or would have been

[7] The Administration's legal rationales for its warrantless wiretapping program have been thoroughly refuted by numerous legal scholars. *See, e.g.,* Letter of Law Professors to Congressional Leadership in Response to Department of Justice Memorandum, *available at* http://www.eff.org/Privacy/Surveillance/NSA/FISA_AUMF_replytoDOJ.pdf.

> intended to protect the United States from a terrorist attack. This section shall apply to all actions, claims, or proceedings pending on or after the effective date of this Act.[8]

As an initial matter, this provision does not just protect telecommunications carriers. Rather, it appears designed to also shield *the government itself* against any lawsuit concerning its "classified communications intelligence activit[ies]" since 9/11. In particular, the proposed immunity would reach any "person" as defined at 18 U.S.C. § 2510(6), *i.e.*, "any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."[9]

Furthermore, this provision's language is not expressly limited to immunity from civil liability. Instead, it seeks to prevent the imposition of *any* "penalty, sanction, or other form of remedy or relief" in *any* legal action in *any* court. Such expansive language could be read to preclude even criminal prosecution. Therefore Section 408 could essentially provide the Attorney General with a stack of blank "get out of jail free" cards for both government agents and telecommunications carriers, representing a complete abandonment of the rule of law when it comes to government surveillance conducted in the name of national security.

That Congress might consider such unprecedented blanket immunity for government agents and the telecommunications carriers that illegally assisted them is all the more shocking considering that neither Congress nor the public even knows what conduct it would be immunizing. Senator Arlen Specter has aptly described Section 408 as "a pig in the poke" since "there has never been a statement from the administration as to what these companies have done."[10] Nor has the Administration come clean about its own conduct, publicly admitting only to the purportedly narrow "Terrorist Surveillance Program" described by the President even as news reports[11] and whistle-blower evidence[12] indicate a much broader program.

Congress must not legislate in the dark, particularly when the rights of so many are at stake. Indeed, it would be unwise for Congress to consider *any* kind of immunity when it has yet to investigate the scope and legality of the Administration's conduct. How many

---

[8] Administration Proposal at § 408(a).

[9] *Id.* at § 408(c)(2).

[10] *See* James Risen, *Legislation Seeks to Ease Rules on Domestic Spying*, The New York Times (April 14, 2007), *available at* http://www.nytimes.com/2007/04/14/us/14fisa.html?ex=1334203200&en=6ce04a0c3e2e2046&ei=5124&partner=permalink&exprod=permalink.

[11] *See supra* note 3.

[12] *See Hepting v. AT&T*, 439 F.Supp.2d at 989 (describing whistle-blower's account of AT&T's dragnet surveillance of Internet communications for the National Security Agency).

Americans have had their privacy violated? How did telecommunications carriers assist in those violations of privacy, and what were they given in return? Congress must conduct a full investigation to uncover the answers to those questions. The public and its elected representatives deserve a full accounting of the Administration's illegal surveillance activities and the telecommunications carriers' participation in that surveillance. Such a full accounting is unlikely ever to occur if every person involved has already been granted a no-strings-attached legislative pardon.

In addition to doing its job by investigating how the Administration has abused its surveillance power since 9/11, Congress should allow the courts to do *their* job by allowing them to adjudicate the legality of that surveillance and the telephone companies' participation in it. The telecommunications industry appears to have assisted the Administration in the greatest mass privacy invasion ever perpetrated on the American people. Americans are entitled to discover the extent to which their privacy was violated and to have a court decide whether the law was broken. Immunity would short-circuit this judicial process, potentially eliminating the courts as a meaningful check on illegal collaboration between telecommunications carriers and the Executive Branch.

Not only is Section 408 designed to ensure that past surveillance by the Administration and its collaborators in the telecommunications industry remains shrouded in secrecy and shielded from judicial review, it would also dangerously increase the risk of *future* illegal collaborations between government and communications providers. Telecommunications carriers' adherence to the law is the biggest practical check that we have against illegal government surveillance. Giving blanket immunity to those carriers, which are the only entities standing between the privacy of countless innocent Americans and government overreaching, sets a dangerous precedent. Section 408 threatens to make Congress' laws a dead letter, eliminated by secret meetings between telecommunications executives and government agents, greased by the promise of similar grants of immunity in the future. There is no reason for Congress to take that risk, as federal law already provides legal protections that adequately protect carriers' good faith cooperation in response to lawful requests by the government.[13]

Instead, in order to fully hold accountable those telecommunications carriers that broke the law and to protect against future law-breaking, Congress should allow those customers whose privacy has been violated to press for the remedies to which they are entitled under statute. Congress rightly established strong civil penalties for violation of FISA and its fellow surveillance statutes,[14] and EFF strongly opposes any legislation that would deprive its clients or any other Americans of the remedies to which they are entitled. Congress' carefully crafted penalties were meant to serve as a strong disincentive against illegal assistance in government surveillance, and to cast them aside now would send a dangerous message: that when the government comes calling and uses

---

[13] *See, e.g.*, 18 U.S.C. §§ 2511(2)(a)(ii) and 2520(d), and 50 U.S.C. § 1805(i).
[14] *See, e.g.*, 50 U.S.C. § 1810 and 18 U.S.C. § 2520(b).

the magic words "national security" or "terrorism," communications providers should feel free to ignore the law.

Finally, to the extent that Congress is concerned by the potential economic impact of such liability on America's telecommunications industry, such concern is wholly premature. Although EFF is confident that its clients will prevail in their current lawsuit against AT&T, that case and other lawsuits against those companies accused of assisting in the Administration's illegal surveillance are still in their early stages. Assuming that the plaintiffs in those suits will ultimately prevail, any award of money damages is likely many years away. Congress should at least allow those cases to continue so that the full scope and legality of the companies' conduct may be discovered and litigated. Then, when the final day of reckoning for the phone companies at last approaches, Congress will have the benefit of a fully developed judicial record to assist it in considering whether the damages to be imposed would be too much—or not nearly enough.

In conclusion, rather than bowing to the Administration's wholly unjustified proposal of blanket immunity, Congress should instead stick to the law that is already on the books. Existing law already strikes a reasonable and bright-line balance between the government's need for industry cooperation in lawful surveillance and the public's need for accountability when industry fails to demand appropriate legal process. The Administration is correct that "[c]ompanies that cooperate with the Government in the war on terror" deserve "our appreciation and protection"[15]—when they do so lawfully. But they deserve neither appreciation nor protection when they break the law and violate the trust of their customers, whether under the claim of national security or otherwise. To the contrary, they deserve to be held to account for their conduct, and indeed must be held to account if we are to prevent secret and unchecked access to the telecommunications networks that carry all of our most private communications.

II. Section 406: Back Door Immunity Through Secrecy

In addition to seeking explicit immunity under Section 408 for government agents and telephone companies that have illegally surveilled Americans, the Administration's proposal also contains provisions, most notably Section 406, that are designed to strengthen the government's argument for a *de facto*, back door immunity based on the so-called state secrets privilege.

Relying on this common law evidentiary privilege, intended to protect from disclosure evidence that will harm national security, the Administration has asserted an astonishingly broad claim: that any lawsuit concerning its warrantless surveillance or the telecommunications industry's participation in such surveillance must be dismissed at the outset. Indeed, it has gone so far as to argue that even if the state secrets privilege did not wholly prevent the cases from being litigated, "[a] court—*even if it were to find unlawfulness* upon *in camera*, *ex parte* review—could not then proceed to adjudicate the

[15] Administration Proposal, Sectional Analysis, p. 60.

very question of awarding damages because to do so would confirm Plaintiffs' allegations."[16] The government argues, essentially, that the state secrets privilege provides complete immunity from suit for any surveillance related to national security. And now, via Section 406 and other provisions of its "modernization" proposal, the Administration is asking Congress to facilitate its attempt to turn this common law evidentiary privilege into a shield against any judicial inquiry into its wrongdoing.

However, Congress has already considered the issue of state secrets in the context of litigation over illegal surveillance, and when passing FISA in 1978 correctly chose not to allow the Executive to use the state secrets privilege as a shield against litigation. In particular, FISA already contains a specific procedure to be followed when the Executive asserts that the disclosure of information concerning electronic surveillance would harm national security. And while that procedure strongly protects national security, it rightly does not contemplate immediate dismissal based on the state secrets privilege.

Instead, FISA provides that if during litigation the Attorney General files a sworn affidavit with the court that disclosure of materials related to electronic surveillance would harm the national security, then the court "*shall*, notwithstanding any other law," review those materials *in camera* and *ex parte*.[17] Furthermore, when reviewing those materials to determine whether the surveillance was lawfully authorized and conducted, the court may if it deems necessary disclose information about the surveillance to the aggrieved person seeking discovery.

This procedure, codified at 50 U.S.C. § 1806(f), reflects several key judgments made by Congress when crafting FISA. First, it reflects Congress' recognition that the legality of surveillance *must be litigable* in order for any of its laws on the subject to have teeth, a recognition bolstered by its creation of a civil remedy in FISA for those who have been illegally surveilled.[18] Second, it reflects Congress' intent to carefully balance that need for accountability with the Executive's interest in avoiding disclosure of information that may harm the national security, and to achieve a "fair and just balance between protection of national security and protection of personal liberties."[19] Finally, it reflects Congress' recognition that the final decision as to what information should be disclosed cannot be left to the Executive's unilateral discretion, but must instead be made by the

---

[16] United States' Reply in Support of the Assertion of the Military and State Secrets Privilege and Motion to Dismiss or, in the Alternative, for Summary Judgment by the United States (*Hepting v. AT&T*, N.D. Cal. Case No. 06-672-VRW, Dkt. No. 245) at p. 20:19-20 (emphasis added), *available at* http://www.eff.org/legal/cases/att/gov_MTD_reply.pdf.

[17] *See* 50 U.S.C. § 1806(f) (emphasis added).

[18] *See* 50 U.S.C. § 1810.

[19] S. Rep. No. 94-1035, at 9 (1976) (discussing § 1806(f)).

courts[20]—courts that both Congress and the Executive trusted could handle sensitive national security information in a reasonable and secure manner.[21]

Now, however, the Administration is unjustifiably asking this Congress to cast aside those carefully considered legislative judgments so it may avoid the judicial scrutiny that FISA demands. Specifically, in Section 406 of its proposal, the Administration asks for the insertion of a new subsection into 50 U.S.C. § 1806, the same section that contains Congress' reasoned procedure for court review and disclosure of secret evidence:

> (l) PROTECTIVE ORDERS AND PRIVILEGES.—Nothing in this section shall prevent the United States from seeking protective orders or asserting privileges ordinarily available to the United States to protect against the disclosure of classified information.[22]

In addition to this provision, other sections of the Administration's proposal are also littered with similar language targeted at bolstering the Executive's assertions of the state secrets privilege.[23] Taken together, these proposed changes represent a bald-faced attempt to avoid the balanced discovery procedure that Congress has previously established, and shield the Administration and those that have cooperated with it from any and all litigation. Yet the Administration has failed to offer any reason why the reasoned judgments made by Congress in 1978 do not still apply with full force. Therefore, and for the same reasons that Congress should reject the immunity proposed in Section 408, it should also reject the Administration's attempt to create a back door immunity based on the state secrets privilege.

III. Section 411: Forum Shopping Through Legislation

Section 411 of the Administration's proposal is the third and final prong in its concerted attempt to stack the deck against Americans seeking redress for being subjected to illegal surveillance. That section would require, *at the Attorney General's discretion*, the transfer "of any case before any court challenging the legality of a classified communications intelligence activity relating to a foreign threat, or in which the legality of any such activity is in issue" to the Foreign Intelligence Surveillance Court

---

[20] Congress explicitly stated that the appropriateness of disclosure is a "decision ... *for the Court to make*[.]" S. Rep. No. 95-701, at 64 (emphasis added); *accord* S. Rep. No. 95-604(I), at 58.

[21] *See* Foreign Intelligence Surveillance Act of 1977: Hearings Before the Subcomm. on Criminal Laws and Procedures of the Senate Comm. on the Judiciary 95th Cong., at 26 (1977) (Attorney General Bell asserting that "[t]he most leakproof branch of the Government is the judiciary . . . I have seen intelligence matters in the courts. . . I have great confidence in the courts," to which Senator Hatch replied, "I do also").

[22] Administration Proposal § 406(2).

[23] *See* Administration Proposal §§ 402, 408(a), and 411(e).

(FISC).[24] By this provision, the Administration obviously seeks for Congress to legislatively enable it to "forum shop" and shuttle all cases regarding its surveillance activities into the court most likely to approve of its conduct. Indeed, the sole role of that court for nearly thirty years has been to routinely approve the Executive's applications for authorization to conduct foreign intelligence surveillance.

The Administration justifies this forum-shopping provision by arguing that only the FISC can be trusted to handle sensitive national security information. Yet as already discussed, Congress and previous administrations have long trusted the regular court system to handle such information responsibly,[25] and the Administration has been unable to point to a single instance in which the judiciary has failed to do so. The Administration's baseless rhetoric about maintaining security therefore cannot justify the diversion of properly maintained lawsuits into a court staffed by judges that are hand-picked by the Chief Justice of the Supreme Court and are accustomed to considering such matters in completely secret and non-adverserial proceedings. Rather, such cases should remain before the fairly and randomly selected state and federal judges that would otherwise adjudicate those disputes in open court—subject, of course, to the carefully balanced FISA procedures discussed previously.

Furthermore, even if the Administration's unfounded security concerns were valid, they would not provide any justification for Section 411's granting of jurisdiction to the Supreme Court for review "by writ of certiori granted upon the petition of the *United States*," while failing to explicitly grant such jurisdiction based upon petitions by the United States' opponents.[26]

Finally, Section 411 would go even further than Section 406 when it comes to strengthening the Administration's ability to abuse the state secrets privilege and bypass FISA's existing procedures, by allowing the *Attorney General and the Director of National Intelligence* to make the final determination as to whether information relating to the national security may be disclosed by the court.[27] Considering the Administration's claims that the FISC—the most secretive judicial venue in the nation—is the most trustworthy court when it comes to responsibly handling such information, this final insult only adds to the grievous injury the Administration's proposal would inflict on the rule of law and the separation of powers.

IV. Conclusion

The Administration's proposal, if passed, will significantly hinder the judiciary's ability to enforce Congress' laws concerning electronic surveillance, giving the Administration brand new excuses in its attempt to avoid judicial scrutiny of its illegal

---

[24] Administration Proposal § 411(a).
[25] *See supra* note 21 and accompanying text.
[26] Administration Proposal § 411(c) (emphasis added).
[27] Administration Proposal § 411(b).

surveillance of Americans in collaboration with telecommunications carriers. For all the foregoing reasons, the Electronic Frontier Foundation respectfully urges this Committee to reject the Administration's current proposal to amend the Foreign Intelligence Surveillance Act.

Statement of James X. Dempsey
Policy Director
Center for Democracy and Technology

before the

Senate Select Committee on Intelligence

Foreign Intelligence Surveillance Act (FISA)

May 1, 2007

Chairman Rockefeller, Vice Chairman Bond, Members of the Committee, thank you for the opportunity to present this written statement for the Committee's hearing on the Foreign Intelligence Surveillance Act (FISA).

On April 13, the Administration offered a bill to make major amendments to FISA. The bill is cloaked in the rhetoric of modernization, but it would turn back the clock to an era of unchecked surveillance of the communications of US citizens, permitting the NSA's vacuum cleaners to be used on all international calls and email of US citizens without court order.

In this statement, we make four main points:

- Of course, technology has changed since FISA was adopted in 1978, but some of those changes have made snooping easier, and in aggregate they have increased the amount of information about our daily lives that is available electronically to the government, thereby requiring stronger, not weaker privacy protections.
- The Administration's bill would go in the wrong direction, by permitting the untargeted warrantless surveillance of all international communications of US citizens. The most important part of the bill would change FISA's definition of "electronic surveillance" to say, in Alice in Wonderland fashion, that the sweeping collection of the international phone calls, email and other communications of American citizens is not "electronic surveillance" and therefore does not require a court order.
- A much narrower set of changes would address the concern that a court order should not be required when the government is collecting foreign-to-foreign communications nor when it is targeting a person abroad who has an incidental number of communications that appear to be with someone in the US.
- In light of press reports that the government has been obtaining massive amounts of transactional records from telephone companies, the Committee should get from the Administration on the public record a clear explanation of the relationship between FISA and the rules for collection of transactional information and stored records.

FISA may need to be updated, but the first step is for the Administration to clearly explain on the public record why FISA is inadequate, which it has failed to do. So far, to the extent that the Administration has actually described issues with FISA, they are ones that could be addressed with much narrower changes. And any changes to FISA should include increased privacy protections, which are clearly needed.

The Administration's proposal is an exercise in cherry-picking: Arguing that FISA is outdated, and claiming to seek consistency and technology neutrality, the Administration proposes to change only aspects of FISA that serve as checks upon its discretion. The Administration accepts unquestioningly those elements of FISA that accord it broad latitude. The result would be a law that is still inconsistent and outdated, but far less protective of the rights of Americans. If there is truly a need to revise FISA, then the reconsideration of Congress' 1978 choices must proceed systematically, not on the basis of a one-sided selectivity. As we explain below, careful consideration should be given to two fundamental elements of FISA: its distinction between wire and radio communications and its distinction between targeted and untargeted surveillance. Consideration should also be given to two areas in which the relationship between FISA and other privacy laws is unclear and may give the Administration unjustified latitude: the relationship between FISA and the criminal statute protecting sensitive transactional data, and the relationship between the FISA and the protections accorded stored communications and records under the Electronic Communications Privacy Act.

I. Changes in Technology Require Stronger, Not Weaker, Standards

The Administration justifies its bill largely on the ground that changes in technology have made FISA outdated. Of course, technology has changed since 1978, but that begs the question of whether FISA should be weakened in response. The Administration never actually explains what technology changes have taken place since 1978, nor does it explain why any such changes justify weakening FISA.

A balanced analysis would show that various technological changes since 1978 require stronger rather than weaker FISA standards.

Perhaps the major change since 1978 that affects FISA is the globalization of personal and economic life, paralleled by the central role of global electronic communications networks in commerce, interpersonal relationships, and the full range of human pursuits. In 1978, it was a rarity for an American citizen to make an international phone call or send an international telegram. In 1978, the signals intelligence activities of the National Security Agency collected some international calls of Americans, but it was pretty rare. Today, interception of communications into and out of the US is likely to pick up the communications of many average American citizens and permanent resident aliens, who are far more likely than in 1978 to have legitimate business dealings overseas or to use the Internet and telephone to keep in touch with relatives overseas. The parent calling her daughter during her junior year abroad, the Chicago lawyer talking to his partner in Brussels, and the small Texas manufacturer with a parts supplier in Vietnam

are all entitled to a reasonable expectation of privacy in their international communications. Far more than in 1978, signals intelligence activity directed at communications entering and leaving the United States is likely to interfere with the privacy of Americans, which means that it must be carefully controlled.

Secondly, while there has been a huge increase in the volume of international communications, there have also been huge increases in computer processing power, making it possible for the government to process more data than ever before. Everything we know about the digital revolution indicates that, on balance, it has been a windfall for the snoopers: More electronic information than ever before is available to the government, and the government's ability to process that information is exponentially greater than ever before. The intelligence agencies are in constant danger of drowning in this information, but they are also constantly improving their processing and analytic capabilities. On balance, the question of volume may be a wash: the agencies have a lot more data to deal with, and they have a lot more ability to handle it. The challenge is daunting, and vital to our national security, but it is hard to see how mere volume justifies lower standards for surveillance of calls to and from Americans in the United States. If anything, the increasing amount of information about our daily lives that is exposed to electronic surveillance calls for stronger, not weaker standards.

A third major technological change is the revolutionary growth of the Internet. Some aspects of the Internet's development, especially the routing of a large percentage of international traffic through the United States, actually make the job of the intelligence agencies much easier in some ways, since they can access foreign-to-foreign communications from US soil. Other aspects of the Internet cited by the Administration – such as General Hayden's assertion that "there are no area codes on the Internet" – may not be entirely accurate and, even if true, require close scrutiny to determine what effect they actually have on electronic surveillance activities carried out in the United States. (FISA only applies to surveillance inside the United States.)

A fourth major change – one alluded to by the Administration -- is the shift to fiber cables as the dominant means of long distance and international carriage. As we will discuss below, the government's argument hinges on the fact that Congress, in 1978, deferred regulating NSA's interception of the satellite portion of international voice communications. Now, the Administration is arguing that radio's temporary exemption should be made permanent and extended to wire communications as well. This is an extraordinary argument: Essentially the Administration is claiming that Americans never had a privacy right for their international satellite calls and that now, just as Americans have become dependent on the Internet to participate in the global economy, they should not have a privacy right for international communications carried by wire either. CDT believes that, if it is time to reconsider FISA's "radio exception," it should be to repeal the exception and extend privacy protections to all of the international communications of Americans, not to eliminate privacy protections across the board.

In addition, the Administration never actually explains why the shift to fiber optics requires a lowering of privacy standards for intercepting the international

communications of Americans. The fact that fiber cables are hard to tap into is irrelevant for purposes of FISA, since, as we noted, FISA applies only inside the United States, where the government does not have to tap into the middle of a cable, because it can compel the cooperation of the service provider at the network operator's switching facility. FISA specifically states that a court order, upon request of the government, shall require any communications carrier to provide "forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance." 50 USC 1805(c)(2)(B).

A fifth technology change merits separate highlighting, and that is the development and deployment of new generations of surveillance-enhancing technology by telephone companies and other communications service providers. Partly, the development of tools to facilitate the interception of advanced technologies is business-driven. Network operators need to be able to trace, isolate and analyze communications to manage their networks, for billing purposes, maintenance, quality control, and security. Other developments are driven by intellectual property concerns, as companies develop means of scanning vast data flows looking for copyrighted material.

Another driver has been legislation like CALEA, the Communications Assistance for Law Enforcement Act of 1994, which specifically requires all communications common carriers to design their systems to make them wiretap friendly. European countries have similar (in some cases more onerous) requirements, and both American standards bodies and the European Telecommunications Standards Institute have developed standards to guide equipment developers. In August 2005, the Federal Communications Commission extended CALEA to broadband Internet access providers and providers of interconnected VoIP (Voice over Internet Protocol) providers.

For these and other reasons, a growing number of companies are developing tools and services to intercept Internet traffic and other advanced communications. One company, for example, notes that its surveillance technology for broadband Internet service providers and ISPs "is highly flexible, utilizing either passive probes or active software functionality within the network nodes to filter out traffic of interest."[1] Cisco has developed what it calls the "Service Independent Intercept Architecture," which uses existing network elements and offers an "integrated approach that limits the intercept activity to the router or gateway that is handling the target's IP traffic and only activates an intercept when the target is accessing the network." http://www.cisco.com/technologies/SII/SII.pdf VeriSign and Aqsacom are two other companies offering comprehensive services for interception of traditional and packet - based network deployments.[2]

---

[1] VERINT Systems, Inc., STAR-GATE for Broadband Data and ISP, http://www.verint.com/lawful_interception/gen_ar2a_view.cfm?article_level2_category_id=7&article_level2a_id=59

[2] http://www.verisign.com/products-services/communications-services/connectivity-and-interoperability-services/calea-compliance/index.html; http://www.aqsacomna.com/us/.

The relevance to intelligence agencies of these tools, developed for business or law enforcement purposes, is a question that merits examination. It is sufficient for our purposes here to note that such tools exist, and they provide a counterweight to the Administration's claims that technology has made its task more difficult. The availability of these tools is particularly relevant to FISA, since, as we noted above, FISA applies only in the US, where the government has the legal authority to compel the cooperation of service providers.

II. The Administration Bill Would Expand Warrantless Surveillance

In order to understand the impact of the Administration bill, it is necessary to appreciate that much of the weight of FISA is carried by its definitions. Most importantly, FISA regulates only "electronic surveillance" as that term is uniquely defined in the Act. If the collection of information fits within the Act's definition of "electronic surveillance," it requires a court order or must fall under one of FISA's exceptions. If the collection of information is ***excluded*** from the definition of electronic surveillance, then it is not regulated by the Act, and the government can proceed without a court order and without reporting to Congress. Therefore, narrowing the definition of electronic surveillance places more activity outside the judicial and Congressional oversight of the Act.

That is precisely what the Administration bill does: It changes the definition of electronic surveillance to exclude from the Act's coverage the collection of a great deal of information about the communications of US citizens that the average person would call "electronic surveillance." Simply put, the changes sought by Administration would authorize large-scale warrantless surveillance of American citizens and the indefinite retention of citizens' communications for future data-mining.

The Administration's language would permit warrantless surveillance of the communications of American citizens in two broad categories:

A. Untargeted Warrantless Surveillance of the International Communications of US Citizens

Under the proposed new definition, all communications to or from the US could be intercepted without a warrant, so long as the government is not targeting a known person in the US.[3] If the government were targeting someone who is overseas, they

---

[3] The new definition of "electronic surveillance" would have two parts: intentionally intercepting international communications of a particular, known person reasonably believed to be in the US, and the acquisition of the contents of communications when all parties are reasonably believed to be in the US. That excludes the collection of the contents of all communications to and from the US so long as the government is not targeting a known, particular person here.

would be able to intercept communications between that person and citizens in the US without a warrant. But the bill goes even further: the government also would not need a warrant if it were engaged in broad, unfocused collection. Under the Administration's bill, the government could intercept all international communications without a warrant, even those originated by citizens and even those involving citizens on both ends.

The bill would permit warrantless surveillance far beyond the President's Terrorist Surveillance Program. Until recently, the Administration consistently argued that it should not need a court order when it is targeting a suspected terrorist overseas calling the US. The problem with the TSP even thus narrowly defined is that, of course, there are two parties to the call, one of whom is in the US and is quite likely a citizen. The person on the phone in the US may be a journalist, an innocent relative, an aid worker, or any other variety of innocent person. Yet under this bill the conversations of those innocent Americans will be intercepted without a warrant.

However, the bill would authorize a program of warrantless surveillance far, far broader than what the President authorized. The President assured the American public that his program was limited to situations where someone from al Qaeda was overseas, calling into the US. The Administration's new bill would authorize warrantless surveillance of all international calls, whether or not there is any reason to believe that al Qaeda is on the line. It would also cover all international calls that originate in the US. Under this bill, for the first time ever, NSA would be able to train its vacuum cleaner on the contents of all international calls, recording every single one, so long as it was not targeting a specific person in the US.

The NSA resents the use of the phrase "vacuum cleaner." It argues that it doesn't want to vacuum up all international calls and couldn't process them even if it did. We use "vacuum cleaner" because the bill would permit without a warrant the untargeted collection of many, many calls, without the particularized suspicion required by the Constitution for government searches.

1. FISA's "Radio Exception" Should Be Repealed - Technology Neutrality Does Not Require Weak Standards

As partial justification for the warrantless interception of all international calls, the Administration's section-by-section analysis and its earlier discussions of this issue refer to FISA's distinction between wire and radio communications, without actually explaining it or justifying why an exception for radio portions of communications should be extended to all communications. We will explain here that the "radio exception" was meant to be temporary, that it is now clearly outdated and that it should be abolished.

When FISA was adopted, it exempted international telephone calls (and other communications) entering and leaving the US by satellite. The Administration unquestioningly accepts this exemption for the radio portion of communications and argues that it should be applied to communications carried by wire, thus exempting from privacy protection all international communications of Americans.

It is clear from FISA's legislative history that Congress intended to consider subsequent legislation to regulate interception of radio communications. The Senate Judiciary Committee's 1977 report on FISA, Rept 95-604, states:

> "The reason for excepting from the definition of 'electronic surveillance' the acquisition of international radio transmissions, including international wire communications when acquired by intercepting radio transmission when not accomplished by targeting a particular United States person in the United States, is to exempt from the provisions of the bill certain signals intelligence activities of the National Security Agency.
>
> Although it is desirable to develop legislative controls in this area, the Committee has concluded that these practices are sufficiently different from traditional electronic surveillance techniques, both conceptually and technologically, that, except when they target particular United States citizens or resident aliens in the United States, they should be considered separately by the Congress. The fact that this bill does not bring these activities within its purview, however, should not be viewed as congressional authorization of such activities." P. 34.
>
> "The activities of the NSA pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the Committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the NSA and the surveillance of Americans abroad raises problems best left to separate legislation. This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely *during the interim period* when the activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed." P. 64 (emphasis added).

The "radio exception" may have been justified in 1978 on the ground that the government was worried about disclosing to carriers the subjects of its interest, or that the carriers were reluctant to cooperate with surveillance, or that the carriers may not have had the ability to isolate the communications of a targeted person or communications instrument. None of those reasons appears valid today. It is clear that carriers are willing and able to cooperate; and the Communications Assistance for Law Enforcement Act of 1994 requires all carriers to build into their networks the ability to isolate the communications to and from specific users. The Administration has offered no explanation as to why changes in technology require it to conducted warrantless surveillance of international calls.

Whatever was the purpose of the radio exception in 1978, there is no reason to apply different standards today. But rather than reconciling the standards by providing satellite communications the same protections that have always applied to wire communications, the Administration would respond by rolling back the protections afforded wire communications and exempting all international communications from FISA, unless the government is targeting a known person in the US. A much better way to make the statute technology neutral is to require a warrant for all interception of communications with one leg in the US.

2. FISA's Dichotomy Between Targeted vs. Non-Targeted Surveillance Should Be Eliminated in Favor of a Court Order Standard for All Methods of Selecting for Processing Communications in Which One Party Is Reasonably Likely to Be a US Person

The Administration's bill, without explanation, perpetuates a distinction drawn in 1978 between the targeted and untargeted interception of communications. In 1978, FISA required a warrant for the acquisition of a radio communication to or from the US only if the contents were acquired by "intentionally targeting" a particular, known US person who is in the US. (f)(1). The Administration would extend this rule to wire communications as well, thus allowing the untargeted acquisition of the communications of a US person.

The question Congress should ask is: What difference does it make to an American that the government collected, analyzed and disseminated his communications without suspecting him of any involvement in terrorism or espionage versus specifically targeting him? The privacy intrusion and the likely harm are the same regardless of whether a person's communications are intercepted because the government was intentionally targeting him or because the government was scanning millions of calls and his were selected as suspicious based on some criteria other than his name. In either case, suspicion may fall on an American and he may face adverse consequences. And in either case, the key question should be how reliable were the selection criteria.

The origins of the distinction between targeting and non-targeting may go back to an issue of major concern at the time FISA was enacted, namely, the "watch-listing" of Americans for NSA surveillance. In the 1960s and 1970s, a practice grew up of watch-listing Americans who were politically active in opposing the Vietnam War or advocating other political positions at odds with the Administration or the views of the leadership of the FBI. One of the purposes of FISA was to prevent the watch-listing of Americans without a court order.

Today, while there are concerns that the Administration has been investigating and harassing political activists, a new concern has emerged: that the data mining and profiling activities of various agencies are causing people real harm in their daily lives. In these cases, the government is not intentionally targeting a particular, known US person. Instead, the government is casting a broad net, using computers to apply selection criteria to oceans of data and selecting out suspicion individuals.

The fact that the selection does not start with a known person does not make the process any less consequential for the privacy of the person whose communications are ultimately selected for scrutiny.

Limiting the definition of "electronic surveillance" to the intentional targeting of a particular, known person seems especially unjustified given the fact that today most selection of communications is computerized, either by the service provider at the direction of the government or by the government itself. Sometimes selection is done by name, sometimes by telephone number or email address or IP address number, and sometimes based on another set of parameters. In all cases, the government should have a solid reason to believe that its criteria will isolate communications that are to or from a foreign power or an agent of a foreign power and that will contain foreign intelligence. In all cases, whether the government uses a name, a telephone number, or a complex set of screens, the process of defining those selection criteria should be subject to judicial scrutiny, based on a finding of probable cause to believe that the communications to be processed will be those of an agent of a foreign power and will contain foreign intelligence.

The current rule and the Administration's bill make no sense, requiring a court order when the government is selecting for interception the communications of a particular, known person but not requiring a court order when the government is selecting communications based on some other criteria. The solution, it seems, is to require a court order for all processing intended to select communications for presentation to a human being. Whether that is a name or a number or a complicated set of screens, the government is selecting for scrutiny the private communications of individuals in circumstances in which those individuals may face adverse consequences, and in our society that is precisely the type of question that should be submitted to prior judicial approval.

3. A Far Narrower Alternative Is Available to Meet the Concerns Expressed by the Administration

The Administration argues that it should be unnecessary to obtain a warrant when it is targeting someone overseas. CDT has been on the record supporting an amendment to FISA that would make it clear that a warrant is not needed when the government is intercepting foreign-to-foreign communications that happen to be available inside the US. An extension of this principle would be to say that the government, when it is collecting foreign-to-foreign communications, should not have to turn off its tap if the overseas target suddenly makes a call to the US.

The simplest and narrowest change would be an exception to the current (f)(2) saying that no warrant is needed when the government, in the course of acquiring the communications of persons outside the US, incidentally collects a communication with a person in the United States. The exception could be narrowly drawn to make it clear that, if the acquisition begins to involve a significant number of communications with a person

in the US, a court order should be required on the grounds that the interception has begun to implicate the rights of an American.

B. Warrantless Surveillance of the Content of Purely Domestic Communications of Citizens

Another section of the Administration bill would allow warrantless interception of the content of the domestic calls of US citizens. Section 402 of the Administration bill would allow warrantless surveillance of the content of purely domestic calls so long as it is "directed at the acquisition of the contents of communications of a foreign power." It is completely unclear what this means. Essentially, all foreign intelligence surveillance is "directed at the acquisition of the communications of a foreign power." The problem is that the person on the other end of the line may be a US citizen, which is why we require a court order.

The proposed change builds on the so-called "embassy exception" to FISA. But that exception was limited to circumstances where it was unlikely that the calls of a US person would be intercepted. The Administration's change would go too far. Basically, it would allow warrantless surveillance of all calls into and out of all embassies, consulates, government-owned corporations like Olympic Airlines, and the US offices of "factions" like the Iraqi Kurds. Many of those calls are to and from US citizens. Indeed, since most foreign embassies and consulates inside the US employ large numbers of US citizens, it is likely that the people on both ends of the calls would be citizens. Under this bill, they could be intercepted without a court order.

As noted, the key language is "directed at the acquisition of the contents of communications of a foreign power." When a foreign national employed by his country's embassy or consulate in the US uses his home phone, is that the "communication of a foreign power?"

FISA contained a narrowly crafted "embassy exception." It was not available if there was likelihood of intercepting the communications of Americans. The Administration's bill would lift that limitation, permitting warrantless surveillance of every school child's effort to get information about France (see http://www.ambafrance-us.org/kids/) and every vacationer's call about visa requirements or immunizations for their overseas travel, let alone every journalist's call to an embassy official.

III. The Committee Should Address Important Issues Regarding Access to Transactional Data and Stored Communications

In an earlier analysis, CDT concluded that the Administration's bill would allow the government, without court order, to intercept information identifying the source and destination of every telephone call and email sent in the US. On closer examination, it appears that our initial analysis was not correct with respect to purely domestic calls, although honestly the relationship between FISA and Title 18 is so circular that it is hard to tell. We urge the Committee to require the Administration to make clear its

interpretation of the relationship between FISA and the rules in Title 18 for the interception of transactional (non-content) data.

Surveillance law has long distinguished between the interception of the content of communications and the interception of dialing or signaling information that indicates who is communicating with whom. The Supreme Court held three decades ago – in cases that look increasingly shaky – that transactional data about calls is not constitutionally protected. Call detail records and Internet records are clearly sensitive, however; they give a full picture of a person's associations and activities. Accordingly, Congress in 1986 required a court order for realtime interception of transactional details about telephone calls, email and other communications (using what are now computer processes but which are still called pen registers or trap and trace devices). 18 U.S.C. 3121- 3127. In criminal investigations, that court order is issued on a very low standard, less than probable cause, and without many of the additional elements of judicial and public oversight accorded to content interceptions. 18 U.S.C. 3123. CDT has long argued that the standard for collection of transactional data should be strengthened.

In contrast, the status of transactional data under FISA has always been unclear. FISA includes a definition of "content" that is broader than the definition of content under the law enforcement wiretapping law. Under FISA, "content" includes information about the existence of a communication or identifying the parties to it, suggesting that a full FISA order is needed to collect transactional data..

In 1998, Congress amended FISA to include a new section authorizing orders in intelligence matters for pen registers and trap and trace devices. 50 U.S.C. 1842-1846. However, Congress did not amend FISA's definition of content, so the Act seemed to be internally inconsistent, defining transactional information as content requiring a full probable cause-based order while also authorizing the collection of transactional information under the lower standard of the pen register/trap and trace section. As far as we know, successive Administrations have not said how they reconcile the conflict.

The Administration bill would eliminate the conflict, by redefining content to exclude transactional information. As we now interpret the Administration's bill, the effect of the changes would be as follows:

18 U.S.C. 3121, which is part of Chapter 206, prohibits the collection of transactional data in real-time without first obtaining a court order issued under 18 U.S.C 3123 (for criminal investigations) or under FISA. However, 18 U.S.C 2511(2)(f) provides that Chapter 206 does not affect the acquisition by the government of foreign intelligence from foreign and international communications utilizing a means other than "electronic surveillance" as defined under FISA. Since the acquisition of non-content from international communications would not be electronic surveillance under the new definitions unless the government is targeting the communications of a particular, known person in the United States, this allows the government to collect transactional information on international calls without a court order. However, 18 U.S.C 2511(2)(f) only applies to foreign and international communications, so 18 USC 2131 would

continue to require a court order for the targeted or untargeted collection of transactional information about domestic calls (as well as for targeted collection of transactional information about international calls).

We urge the committee to confirm this interpretation with the Administration on the public record, especially that 3121 requires a pen/trap order under 50 USC 1842-1846 for collection of transactional information on all domestic calls, whether the information is collected on a targeted or untargeted basis.

Of course, this allows the government access without a court order to all transactional data for international calls when the government is not targeting a particular, known person in the US, even though such data gives a rich picture of the associations and activities of US citizens. In addition, even with respect to domestic calls, FISA sets a very low standard, merely requiring the government to certify (with no factual explanation) that the information likely to be obtained is foreign intelligence not concerning a US person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities. CDT believes that this standard should be raised, to at least require the government to offer some basic facts reasonably supporting the claim that the surveillance will yield foreign intelligence or information relevant to an ongoing investigation of international terrorism or clandestine intelligence activity.

CDT also urges the Committee to determine whether the Administration reads 50 USC 1842 as requiring particularity. That is, does FISA's pen/trap standard, as amended by the PATRTIOT Act, require the government to obtain pen/trap orders only on specific phone lines or email accounts used by particular persons, or has the government been obtaining FISA pen/trap orders authorizing the collection of transactional data pertaining to many individuals? Judicial oversight would be largely meaningless if the government could get pen/trap orders without particularity, i.e., without focusing on a particular individual.

The Committee should also explore reports that the Administration has been obtaining large quantities of transactional data in stored formats. If the telephone companies are turning over large volumes of transactional data on a regular basis, that would be a major evasion of the provisions of 18 USC 3121 and 50 USC. It seems to make little difference between recording massive amounts of transactional data inrealtime versus acquiring that data in stored form soon after the communications.

Finally, we note that the Administration bill seems to preserve part of the inconsistency of current law, for the new (f)(1) requires a full probable cause-based court order to collect any "information" about the communication of a particular, known person who is reasonably believed to be in the United States. Thus, the Administration bill would set a higher standard for the targeted use of pen registers and trap and trace devices to collect transactional data in some national security cases than would be required in criminal cases.

IV. What Protection Do "Minimization Procedures" Provide?

The draft bill and the explanatory statement point to "minimization procedures," which are secret rules written by the Attorney General governing the acquisition, retention and dissemination of information. We have no doubt that NSA employees take minimization very seriously, but the concept itself offers little protection. Minimization does not mean that the government cannot collect, retain or disseminate information about US persons. To the contrary, minimization procedures allow the collection, retention and dissemination of "foreign intelligence" regarding US persons.

Since the main purpose of intelligence gathering is to gather foreign intelligence – since the intelligence agencies have no reason to be collecting or disseminating anything that is not foreign intelligence whether it relates to a US person or not -- the minimization rules offer little added protection. The concern is not that the intelligence agencies will be collecting information about the extramarital affairs of Americans. The concern is that the intelligence agencies can collect and disseminate ambiguous, incomplete and potentially misleading information about the foreign travels, relationships and activities of Americans that may relate to some aspect of US foreign policy. Whether such collection and dissemination is appropriate in any case should be a matter for judicial review, not left to secret minimization rules written by the Attorney General.

The bill also cuts back on the minimization requirement. Under current law, if the government, acting without a warrant under Section 102(a) of FISA, obtains the communications of a US person, those communications cannot be disclosed, disseminated or used, and the government must destroy them within 72 hours unless the Attorney General obtains a court order or determines that the information indicates a threat of death or serious physical harm. The Administration bill would permit unrestricted retention and use of the communications of US citizens obtained without a warrant under the vastly expanded Section 102. This change is especially important in light of the changes made to Section 102(a), which include new authority for warrantless surveillance of domestic calls involving US citizens.

V. Reducing Judicial Oversight by Reducing the Detail in FISA Applications

The bill would cut back on the information the government is required to include in its applications to the FISA court. Some of the information the bill would cut from the government's applications is useful to the court in determining if the surveillance is reasonable. Without this information, it will be hard for the court to issue an order specifying the scope of permitted surveillance. Given what we have learned about the tendency of intelligence agencies to cut corners (for example, the FBI's issuance of emergency records demands when no emergency existed), this does not seem to be the time to cut back on the amount of information provided to those responsible for checks and balances.

The alternative, bipartisan legislation introduced by Senators Feinstein and Specter, S. 1114, appears to take a far more measured approach than the radical revisions the Administration has urged.

VI. The Administration Bill Would Deprive Communications Companies of the Certainty They Deserve When Presented with Government Surveillance Requests

Effective government surveillance depends on the prompt cooperation of the operators of communications networks. It is appropriate that telephone companies and other operators of communications networks should be required to cooperate with court-approved electronic surveillance. However, carriers should not be placed in the position of having to evaluate the legality of each government request. The court order provision gives carriers the certainty they deserve: if the government presents a court order, the carrier must comply and will be protected from liability even if the order was improperly obtained. If the government does not have a court order, the carrier can safely and confidently decline to cooperate. What is crucial is that those companies should be afforded clear rules. Carriers should not be left guessing as to when to cooperate.

Section 408 of the bill would upset this balance and deprive communications carriers of the certainty they deserve. It would grant immunity to certain carriers who cooperated with government surveillance requests in the absence of a court order. The change would place those carriers and all other carriers in an impossible position during the next crisis: If the government approached them with a questionable request, should they cooperate in the expectation that they would later get immunity, or should they resist in the face of government claims that national security was at stake? The provision diminishes the meaning of the court order process as a means of affording companies protection.

VII. Conclusion: Congress Should Proceed Cautiously and Engage in an On-the-Record Exploration of the Issues Raised by the Administration's Proposals

There is a long, secret history to the Administration's proposed bill. The Administration states that its proposed language has been under development for more than a year. The issues addressed by the bill have been debated intensively inside the Administration since soon after 9/11 and were percolating before then. Congress has not been part of those debates and should not simply accept the Administration's proposals. It should move cautiously and take time to understand the issues and to consider the impact of the changes sought by the Administration on the rights of the American people.

The first step is for Congress to get on the public record the full story on the Administration's warrantless surveillance activities. The proposed bill would give immunity to the telecommunications carriers involved in those activities and thus terminate the various pending lawsuits, which may be one of the best means of getting to the bottom of the Administration's violations of FISA.

Before going forward with any amendments to FISA, Congress should hold public hearings to examine what problems, if any, the Administration has with the current law. Those hearings can be held without jeopardizing national security. Based on such hearings, Congress can identify which issues—if any-- raised by the Administration are real and require narrowly focused changes . At the same time, Congress should address the ways in which FISA should be strengthened to provide better privacy protection. In holding those hearings, Congress should distinguish between the criticality of the mission of the National Security Agency and the weak standards proposed in this bill. Of course, when al Qaeda is calling the US, we want to be listening. The question is, what should be the legal standard when a US citizen is on the other end of the call? And should the government be able to conduct surveillance when it has no reason to believe al Qaeda is on the line?

CDT urges the Committee to reject this sweeping proposal. We look forward to working with the Committee to craft any needed FISA amendments on a narrow and balanced basis.

STATEMENT OF BRUCE FEIN

BEFORE THE SENATE INTELLIGENCE COMMITTEE

RE: FOREIGN INTELLIGENCE SURVEILLANCE MODERNIZATION ACT OF 2007

MAY 1, 2007

Dear Mr. Chairman and Members of the Committee:

I am pleased to share my views on the Foreign Intelligence Surveillance Modernization Act of 2007 (FISMA). It represents a grasp for spying authority worthy of Big Brother and George Orwell's 1984. The government has not come close to demonstrating a national security need that would justify the alarming encroachments on the right to be left alone—the liberty most cherished in civilized nations—that would be effectuated by the proposed legislation.

The revolutionary idea behind the Declaration of Independence was that the chief end of the state is to make men and women free to develop their faculties and to pursue wisdom and virtue, not to aggrandize government or to build a world empire. Freedom was to be the rule, and government encroachments were to be the exception and to be justified only by a serious showing of need. That philosophy finds explicit expression in the Fourth Amendment, which prohibits unreasonable searches and seizures, and authorizes warrants issued by independent magistrates only when probable cause to suspect mischief is established.

The United States Constitution aimed to secure individual freedoms through a system of checks and balances. The Founding Fathers understood that men are not angels; that ambition must be made to counteract ambition; that "trust me" is an untrustworthy protection of liberty; and, that unchecked or absolute power invariably occasions oppression or abuses. Thus, the Constitution abhors endowing any branch of government with power that escapes vetting by co-equal branches.

The United States recklessly experimented with unchecked executive power to gather intelligence from President Franklin D. Roosevelt through President Richard M.

Nixon. Its history is a history of abuses: illegal mail openings; illegal interceptions of international telegraphs; misuse of the National Security Agency (NSA) for non-intelligence purposes; the gathering of political intelligence to harm political opponents under the bogus umbrella of national security intelligence, etc. The chronicles of the Church Committee should be chilling to any free society.

The Foreign Intelligence Surveillance Act of 1978 was the child of this ignoble experiment with executive branch supremacy. Generally speaking, it requires judicial warrants to target American citizens or permanent resident aliens for electronic surveillance or physical searches based on probable cause to believe that the target is an agent of a foreign power or international terrorist organization or lone wolf terrorist. There are exceptions for emergencies and for war. Minimization requirements prevent the maintenance of a data base on individuals inadvertently heard in the course of a valid surveillance. FISA has been amended six times since 9/11 to adapt to the heightened danger and advances in communication technologies. As recently as July 31, 2002, the Justice Department informed the Senate Intelligence Committee that FISA operated with flexibility and nimbleness that enabled the thwarting of terrorist plots in the bud. Accordingly, the Department opposes lowering the evidentiary threshold for obtaining a FISA warrant because of constitutional scruples.

Neither the 9/11 Commission nor any other reputable organization or individual has maintained that the 9/11 abominations would have been thwarted if FISA had never been enacted.

President George W. Bush, nevertheless, instructed the NSA in the aftermath of 9/11 to target American citizens on American soil for electronic surveillance on his say-

so alone in contravention of FISA. A federal district court has ruled the NSA's domestic warrantless surveillance program unconstitutional, and an appeal is pending in the United States Court of Appeals for the Sixth Circuit. Further, Attorney General Alberto Gonzales recently obtained some type of FISA warrant for the NSA's spying program, although the details have not been made public or shared with Congress generally. In any event, the Bush administration has been not provided a crumb of evidence that the NSA's flouting of FISA yielded any non-trivial foreign intelligence that could not have been obtained in compliance with FISA. If the evidence existed, it seems certain that the administration would have leaked it to the press to justify the NSA's circumvention of FISA and apparent contravention of the Fourth Amendment.

The FBI's recurring misuses or misapplication of its power to issue national security letters under the Patriot Act demonstrates the inherent tendency of bureaucracies and the executive branch to abuse unchecked intelligence authorities.

The foregoing principles and history inform my critique of FISMA. Section 401 would broaden the definition of a foreign agent to include non-U.S. persons in the United States who may possess, control, or receive foreign intelligence information. That broadening would bring within its sweep virtually every visiting non-citizen because foreign intelligence includes any type of cultural, social, economic, or political knowledge in foreign lands that might be useful in crafting United States diplomacy. Only persons with a lobotomy would be excluded. The government has made no showing of why the broadening would be more than trivial to the national security. The broadening to include persons suspected of complicity in the proliferation of WMD seems unobjectionable.

Section 401 would also sharply narrow the definition of electronic surveillance to render FISA largely meaningless. Under the proposed new definition, the NSA's blanket interception of every conversation or email of every American on American soil without intending to conduct surveillance against a particular known person would be outside the scope of FISA regulation. The government has not shown why this wholesale assault upon Fourth Amendment privacy values would be more than trivial to the national security.

Section 401 would also exclude from FISA government interceptions of emails or conversations of United States persons when the possibility that one of the communicants is outside the United States is conceivable, which is virtually always the case. The government has made no showing as to how this evisceration of FISA would advance the national security in a non-trivial way.

Section 408 would establish absolute immunity for any person who assisted the intelligence community in any way between 9/11 and the effective date of FISMA—even when the person knew the assistance was illegal. Under military law, a common foot soldier is obligated to disobey a clearly illegal order. There seems no reason to resist applying at least the same standard to civilians involved in the war on international terrorism. It would be a terrible blow to the rule of law to shield from redress conduct known to the perpetrator to have been lawless. The customary practice is to provide a good faith defense to ostensible Good Samaritans, and to impose liability only when the alleged culprit violated "clearly established" constitutional norms. That should be the standard of section 408.

The Constitution is not a suicide pact. But it requires that every departure from freedom be justified by government necessity proven either by experience or inexorable logic. The government has failed to satisfy that benchmark in several provisions of the FISMA. The Bush administration should be applauded, however, for tacitly conceding in proposing FISMA that Congress is entrusted with power to regulate the collection of foreign intelligence. Its previous unyielding position had been that FISA or any other congressional attempt to restrain in any way the President's gathering of foreign intelligence was unconstitutional.

WASHINGTON
LEGISLATIVE OFFICE

American Civil Liberties Union
Statement for the Record

Before the Senate Permanent Select Committee on Intelligence
Regarding the Department of Justice's Proposed Foreign Intelligence Surveillance Act Amendments

Submitted by Caroline Frederickson,
Director, ACLU Washington Legislative Office

May 1, 2007

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

CAROLINE FREDRICKSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

On behalf of the American Civil Liberties Union, and its hundreds of thousands of activists and members, and fifty-three affiliates nationwide, we urge you in the strongest terms to oppose legislation drafted by the Department of Justice ("DOJ") that would effectively pardon telecommunication companies for illegal behavior over the last five years and rewrite the Foreign Intelligence Surveillance Act ("FISA") to facilitate further warrantless surveillance on American soil.[1]

Only a few short weeks ago this Congress was finally informed about the DOJ's use of National Security Letters ("NSLs") and found that this power – no longer limited to collecting information on terrorists – is being abused to collect vast amounts of data on innocent Americans that is stored indefinitely in massive federal databases accessible by tens of thousands of users. Instead of contemplating ways to exponentially increase those powers, this Congress should be figuring out ways to rein them in, protect constitutional rights, and focus our antiterrorism resources on suspected terrorists.

While the Administration claims that the changes it proposes to FISA would "modernize" it, they would better be described as changes to gut the judicial oversight mechanisms carefully crafted to prevent abuse, while expanding the universe of communications that can be intercepted under FISA. They would allow the intelligence community to return to the tarnished practices of the 1970's and earlier, when warrants were largely optional and abusive spying

[1] FISA Modernization Provisions of the Proposed Fiscal Year 2008 Intelligence Authorization, Title IV, *available at* http://www.fas.org/irp/news/2007/04/fisa-proposal.pdf.

was not limited to subjects who had done something wrong. In fact, despite numerous hearings about "modernization" and "technology neutrality" over the last year, the Administration has not publicly provided Congress with a single example of how current standards in FISA have either prevented the intelligence community from using new technologies or proven unworkable for the personnel tasked with following them. Congress should not approve sweeping new authorities without such a showing by the Administration.

Granting Immunity to the Companies Who Facilitated Illegal Spying Is Inappropriate.

We are disappointed and very concerned that the first hearing in this Congress to address five years of illegal spying would consider a legislative, congressional pardon for the telecommunication companies that broke the law. Congress' priority should be a full and public airing of the government's illegal spying, including determining exactly how many people the government and telecommunications companies spied on for five years and what is now being done with records of those phone calls; holding those who broke the law responsible; and then fashioning a response to make sure these grave violations of privacy never happen again.

This Committee should be holding a hearing to determine how to contract, rather than expand, the government's illegal spying to bring it into conformity with the law and Constitution; yet the Administration's proposed bill proposes an unwise new power grab. For example, sections 408 and 411 attempt to terminate all pending and future actions against the NSA's warrantless wiretapping in any court anywhere, except for a FISA court whose judges are handpicked by the Chief Justice. The US District Court in the Eastern District of Michigan recently ruled that the president's program to wiretap Americans without warrants is illegal and unconstitutional. The Administration, having lost in one forum, asks Congress to give it a new one.

The Administration's proposed bill is objectionable because it eliminates independent court review of the Administration's past and future spying and eavesdropping requests. The proposed bill would allow the administration to rip that case from that court's jurisdiction, and ship other federal and state court challenges off for secret hearings and proceedings before the FISA Court of Review, which has handled only one case in nearly 30 years. And, only the government would be allowed to appeal to the U.S. Supreme Court to seek review of any adverse ruling by that Court. The bill abrogates rights granted under state law as well, by stopping state law enforcement and regulatory agencies from enforcing local consumer privacy laws that may offer more protection than federal law. Beyond the mandatory transfer provision, the bill allows companies to assert immunity for complying with secret requests of the AG under provisions that state that:

> No action shall lie or be maintained in any court, and no penalty, sanction or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities or any other form of assistance during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act....[2]

This exemption is both overbroad and unwise.

If Congress grants these companies immunity for violating longstanding privacy laws, what incentive will they have to follow them in the future? Without consequences, these laws ring hollow, and end up being a mere suggestion instead of a mandate or bright line requirement. For nearly 30 years, FISA has included a clear liability and immunity scheme that creates bright lines for telecommunication companies: if they turn over private information in response to a legal demand from the government, they are 100 percent immune from any liability. However, if they cut a side deal with the executive branch in an attempt to bypass the duly enacted laws of this Congress, they are liable to the consumers whose privacy they have betrayed. If our government wants to "improv[e] the way the United States does business with communications providers," as the DOJ claims on the fact sheet it conveyed to Congress with its legislative proposal,[3] it should return to the days of clear cut requirements, instead of enticing those providers to break the law with the promise of a congressional pardon after the fact.

Finally, this rush to retroactive immunity for an entire industry in the absence of full and thorough airing of the facts is unprecedented. Numerous leaders in this Congress have promised to investigate the President's illegal Terrorist Surveillance Program. It is highly unlikely those investigations will yield any useful information if Congress starts the process giving the companies a get out of jail free card.

Changing Technical Definitions in FISA to Undercut the Warrant Requirement of the Fourth Amendment.

Sections 401 and 402 of the proposed Administration bill alter FISA's current definitions of "electronic surveillance" to greatly reduce the number

---

[2] *Id.* at § 408 (a).

[3] FACT SHEET: TITLE IV OF THE FISCAL YEAR 2008 INTELLIGENCE AUTHORIZATION ACT, MATTERS RELATED TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, Office of Public Affairs, Apr. 13, 2007.

and scope of spying activities that are subject to court review. The DOJ's Office of Public Policy, claims these changes are necessary "to account for the sweeping changes in telecommunications technology that have taken place."[4] This includes making FISA "technology neutral" by deleting the longstanding requirement that all wire communications into and out of the U.S. are accessed only on the basis of a warrant.[5]

These changes have absolutely nothing to do with "modernizing" FISA – rather, they substantially and unconstitutionally declare whole categories of communications exempt from the warrant requirement, namely, 1) international phone calls, even when made in the U.S. by a U.S. person, and 2) phone calls collected as a part of a general dragnet, as long as no one U.S. person was targeted. Technology may have changed, but the Fourth Amendment has not. Except for a few very narrow circumstances, warrants are required to listen to phone calls or otherwise access the content of a communication and we ask this committee to make sure that requirement remains a cornerstone of FISA.

The Justice Department has claimed that this proposal restores the "original intent" of the law but the legislative history makes clear that Congress intended FISA to prevent the National Security Agency ("NSA") from engaging in just the sort of electronic dragnet this bill permits. The Church Committee's discovery that the NSA was improperly monitoring millions of international telegrams to and from Americans and U.S. businesses through "Operation Shamrock" led a bipartisan coalition in Congress to enact FISA to prevent future presidents from intercepting the "international communications of American citizens whose privacy ought to be protected under the Constitution" ever again. See, Book III of the Final Report on Intelligence Activities and the Rights of Americans, Apr. 23, 1976, at pp. 735-36.

This draft proposal would also allow the NSA to acquire Americans' private e-mail messages if the government says it does not know that "the sender and all intended recipients are located within" the U.S. This provision would authorize the NSA to vacuum up all of the international e-mails of Americans. The NSA would likely capture purely domestic e-mails in this program as well because, as Central Intelligence Agency Director General Michael Hayden said, "there are no zip codes on the world wide web." For example, if an American in New York City sends an email to his sister in San Francisco, that communication could be intercepted without a warrant because it went through Canada. This bill would allow the NSA to keep these "accidentally" captured communications. Once "lawfully" acquired under

---

[4] *Id.*

[5] Nearly identical language was introduced in the House and Senate last Congress. H.R. 5825, 109th Cong. (2nd Sess. 2006); S. 3931, 109th Cong. (2nd Sess. 2006).

this authority, the administration could — and most likely already does — interpret the statute to allow the NSA to target any particular American's communications from such a dragnet for data mining, analysis, or dissemination. Because this activity is not considered "electronic surveillance" under the new language proposed in this bill, a substantial number of innocent Americans' private conversations would be exempt from the oversight of the court and congressional reporting. While the bill retains FISA's minimization rules, those rules only apply to "electronic surveillance" which is redefined in this draft bill to exclude innocent Americans' international conversations and e-mails. Thus, this supposed protection is illusory.

The proposal also amends FISA to require a warrant only when a surveillance device acquires conversations by "intentionally directing the surveillance" at a specific U.S. person. Under the Justice Department's draft bill, if the NSA's surveillance devices — as distinguished from its data mining devices — are directed at wholly domestic conversations but not at a specific American, no warrant need be sought. FISA's targeting language is a shield against sweeping up the conversations of innocent Americans. The proposed language turns this into a sword to cut down statutory protections for our Fourth Amendment rights.

Stripping Non-citizens – And Anyone Who Comes Into Contact With Them -- of the Protection of a Warrant.

Section 402 greatly reduces the protection against government spying on non-U.S. persons and puts at risk the privacy of any U.S. persons who may come into contact with them. Current law has a narrow exception to the warrant requirement that allows the Attorney General to issue wiretap orders for 1) communications that are exclusively between foreign powers, such as contact between embassies and foreign countries, or 2) technical intelligence from property under the exclusive control of a foreign power, when either of these activities has "no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party."[6] Section 402 strips both the requirement that communications or technical intelligence be exclusively between or on the property of a foreign power, and the requirement that there be no substantial likelihood that a U.S. person be caught up in the surveillance. This greatly increases the chances, and in fact expressly allows, that a U.S. person may have his or her communications scooped up in surveillance of foreign powers.

This bill even expands the definition of "agent of a foreign power" to include anyone in the U.S. who is not a citizen, lawful permanent resident or company incorporated in the U.S. who "is expected to possess, control,

[6] 50 U.S.C. § 102 (a).

transmit or receive foreign intelligence information" in the U.S. This is dangerous because FISA's definition of "foreign intelligence" is not limited to international terrorism but includes information about the "national defense," "security," or "conduct of the foreign affairs" of the U.S., which has been construed to include trade matters. All foreign journalists and foreign-owned media companies, financial institutions, airlines, telecommunications companies, or Internet Service Providers (ISPs) could be considered "agents of a foreign power" whose communications could be seized without any suspicion of wrongdoing, just because they all can reasonably be expected to "possess," "transmit" and "receive" foreign intelligence information within the United States. Communications of many foreign businesses in the U.S. transmit or hold information that involves foreign affairs, particularly foreign media and financial institutions. All the Administration would have to show to get a FISA order to search or wiretap these entities for an entire year is that these entities possess such information, not that they have done or are expected to do anything improper.

Expands Disclosure of Information Obtained in Warrantless Searches of Homes and Businesses

Section 409 makes dangerous changes to the provisions of FISA that allow the Attorney General to authorize physical searches in the absence of a warrant in times of emergency.[7] First, it expands the period of time the Attorney General has to search a home without judicial approval from three days to a full week.

Second, and most importantly, section 409 allows the Attorney General to share information obtained in emergency physical searches even when the court later finds that the search was wrongly conducted. The current emergency search statute bars the government from using or distributing any information or evidence collected during an emergency search if subsequent judicial review denies the retroactive warrant.[8] The only exception is when that information "indicates a threat of death or serious bodily harm to any person."[9] This ban on later use operates to deter the government from conducting "emergency" searches in cases where no true emergency exists or when the government knows it will not be able to meet the subsequent warrant requirements.

---

[7] 50 U.S.C. § 1821, et. Seq.

[8] 50 U.S.C. § 1824 (e) (4).

[9] *Id.*

Section 409 greatly expands the threat of death exception and allows the government to use and disseminate this information or evidence, which in retrospect was wrongly collected, based on the incredibly low standard that it "*is significant foreign intelligence information.*" FISA already defines "foreign intelligence information" extremely broadly, including any information that allows the United States to protect itself against a potential attack or international terrorism.[10] This is so broad that the government would be authorized to retain, use and distribute virtually all information it collects under the guise of an "emergency" physical search, even if a court later finds that there was no basis whatsoever in the law to claim emergency circumstances.

If these changes are enacted, the government will have no incentive to limit its use of this authority. Some may claim such a scenario is highly unlikely, and that our intelligence professionals should be given the benefit of the doubt. However, the Inspector General's report recently confirmed that the FBI routinely lied about emergencies to access telecommunication records. This section will simply grant legislative approval of that practice – except in far more serious situations: the highly sensitive searches of homes, businesses, cars or other physical space. Concerns about the DOJ concocting emergencies can no longer be dismissed as fantastical, paranoid hyperbole. The American public has recently learned from the DOJ's Inspector General that fabricated "emergencies" led to the issuance of so-called "exigent letters" where no emergency existed. It would be unwise for Congress to follow that revelation of abuse of authority with a new grant of authority to use information gathered from searches after it was determined the search was improperly grounded. If Congress authorizes such use of wrongly gotten search results, how long will it be before a subsequent Inspector General's report documenting the abuse of such an authority to conduct fishing expeditions?

Other Deletions of Checks and Balances.

---

[10] 50 U.S.C. § 1801(e) defines "foreign intelligence information" as:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.

A number of other provisions in this proposed bill appear to have no purpose other than to reduce the checks and balances in FISA. Section 405 extends the maximum time period for a FISA warrant for a non-U.S. citizen from 120 days to one year, and extends the duration of emergency wiretap orders that allow the government to surveil suspects without prior judicial review from 72 hours to one week. Section 410 extends the period of emergency trap and trace orders from 48 hours to one week. Again, the Administration has provided no evidence that the current time limits are unworkable. While the Justice Department has requested "flexibility," and justifies less court review under the guise of saving time, periodic and timely review of orders is necessary to ensure that the government does not continue spying on people in the absence of some evidence that the person is a terrorist.

Sections 404 and 405 further reduce judicial oversight. They amend the application and order process so that the DOJ no longer need provide either meaningful descriptions of key intelligence activities, such as "the nature of the information sought and the type of communications or activities to be subjected to the surveillance,"[11] or "a statement of the means by which the surveillance will be effected and a statement whether the physical entry is required to effect the surveillance."[12] Instead, if enacted, the DOJ would be empowered to simply produce a summary, reducing the information a court may use to determine whether certain types of surveillance are appropriate.

Conclusion: this Committee Should Hold Hearings to Document and Reform the Government's Abusive Spying and Should Refrain from Adopting the Administration's Proposed Legislation.

The proposed amendments to FISA do not "modernize" intelligence-gathering activities. They simply declare certain communications outside of the warrant requirement and reduce judicial oversight, in violation of the Fourth Amendment. In light of recent revelations that the government is gravely abusing the authorities it already has, allowing this exponential increase in spying authority would not only be unconstitutional, but irresponsible. We urge you to resist any such expansion.

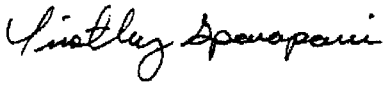
---

[11] 50 U.S.C. § 1804 (a) (6).

[12] *Id.* at § (a) (8).

Sincerely,

Caroline Fredrickson
Director, Washington Legislative Office



Timothy Sparapani
Legislative Counsel for Privacy Rights

David S. Kris
800 Connecticut Avenue, NW
Suite 800
Washington, DC 20006

May 1, 2007

The Honorable John D. Rockefeller IV
Chairman
Select Committee on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Christopher S. Bond
Vice Chairman
Select Committee on Intelligence
United States Senate
211 Hart Senate Office Building
Washington, D.C. 20510

Dear Mr. Chairman and Mr. Vice Chairman:

In response to a request from your staff, I am writing with my comments on the Foreign Intelligence Surveillance Modernization Act of 2007, which I understand was submitted to Congress by the executive branch as proposed Title IV of the Intelligence Authorization Act for Fiscal Year 2008. The proposal is 66 pages long and includes several very significant changes to the Foreign Intelligence Surveillance Act (FISA). Although I have had ample time to consider the meaning of current FISA, my comments on the government's proposal are the product of a very few days, and are necessarily tentative.[1]

I have three general reactions to the government's proposal. First, with few exceptions (changes to the definition of "agent of a foreign power"), it does not expand the range or type of surveillance that the government may lawfully conduct. In other words, it is not primarily designed to fill any gaps in available coverage. In any event – and this is my second reaction – the proposal substantially shifts the power to authorize surveillance from the judicial to the executive branch. In other words, it contracts the jurisdiction of the Foreign Intelligence Surveillance Court (FISC), and expands the authority of the Attorney General and the National Security Agency (NSA). Third and finally, I worry that this proposal may have unintended consequences in a statute as complex as FISA (although I concede that I have not had much time to review the proposal or to consider the ways in which its various elements work together).

In my opinion, Sections 401(b) and 402 are by far the most significant provisions in the government's proposal. I focus much of my attention on them. Where possible, however, I also discuss other provisions in the proposal. Following a brief summary of my views, which is set out immediately below, I try to describe and explain the law as it is today, and then address how I believe the law will change if the government's proposal is enacted. I do not significantly confront the policy arguments for or against the government's proposal; in part because of time constraints, my main purpose now is to *explain* what I think it means.

SUMMARY

Section 401(a). Section 401(a) of the government's proposal would amend the definition of "agent of a foreign power" in FISA to include any non-U.S. person who "is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States," if the government certifies that the foreign intelligence information is "significant." This provision appears to me to be a catch-all, and the Committee may want the government to identify one or more real or hypothetical cases to justify it. I would not be surprised if such examples can only be provided in closed session. Assuming the provision is needed, I believe the Committee should consider carefully what it means for "foreign intelligence information" to be "significant," and consider how that adjective will work with the current syntax of the definition. Finally, because this provision merges the probable-cause and purpose provisions of the statute, I also believe the Committee should consider limiting its use to situations in which the government cannot satisfy the other definitions of "agent of a foreign power."

Section 401(b). Section 401(b) of the government's proposal would amend the definition of "electronic surveillance," on which the entire regulatory framework of subchapter I of FISA depends. This is major surgery on a very complex statute, and it may well be necessary, but it definitely should not be undertaken lightly. I have tried, in the body of this letter, to review extremely carefully the meaning of current FISA, the ways in which that meaning will change if the government's proposal is enacted, and the implications of such change for various forms of actual surveillance activity. But I am four years out of government, and national security is just my hobby. The Committee may want to request a far more authoritative and comprehensive analysis from the executive branch, to help explain *exactly* how the government's proposal will affect surveillance operations, and protections for privacy and civil liberties, as well as the reasons why change is needed or desired. This is an area in which the tiniest technical details can make an enormous difference.

I have three specific questions about Section 401(b). First, what does it mean to "intentionally direct[] surveillance at a *particular, known* person" under proposed Subsection (1) of the definition of "electronic surveillance"? In particular, does this language exclude wide-ranging or "driftnet" surveillance, on the theory that the target of such surveillance is *all* persons (or persons in general), rather than any "particular, known" person? If not, what does the government say to changing the language to refer to "any person or persons" instead of a "particular, known person"?

Second, why does proposed Subsection (1) refer to the reasonable expectation of privacy enjoyed by "that person" – the "particular, known" target of the surveillance – rather than the traditional formulation, "a person"? What is the government's view on whether foreign governments and non-U.S. persons enjoy Fourth Amendment rights while inside the United States? How will the use of "that person" affect surveillance of them?

Third, although I cannot discuss them here, there are several technically complex – and arguably metaphysical – questions about the application of this provision to e-mail. The Committee may want to discuss this with the government in a closed session.

Section 402. Section 402, which would amend 50 U.S.C. § 1802, is also a far-reaching proposal. It authorizes surveillance of certain foreign powers without judicial review. In 1978, the absence of judicial review was justified by the fact that the provision governed "a class of surveillances, otherwise within the scope of the bill, where there was little or no likelihood that Americans' Fourth Amendment rights would be involved in any way."[2] Under the government's proposal, that would no longer be the case. Thus, the main policy question is relatively clearly presented.

Congress should also request a more complete explanation of proposed 50 U.S.C. § 1802A, which would also be enacted by Section 402 of the government's proposal. How does this provision relate to the narrowing of the definition of "electronic surveillance" in Section 401(b) of the proposal? How, if at all, would it affect the (judicial or non-judicial versions of) the Terrorist Surveillance Program (TSP) and other existing or contemplated surveillance programs? Finally, are one-year periods of unilateral executive branch surveillance of U.S. persons "reasonable" under the Fourth Amendment?

Section 404. The most significant aspect of Section 404 of the government's proposal is that it allows the President to name *any* federal officer as the certifying official for a FISA application. Under current law, only a Senate-confirmed official may be named. This is an important change because, while it offers obvious operational benefits, it risks denigrating the significance of the certification.

DISCUSSION

The following paragraphs present my comments on current law, and the government's proposal, in more detail. **For ease of reference, given the length and density of the discussion, I have presented what I think are the most important points in bold text.**

Section 401(a)

Section 401(a) of the government's proposal would amend the definition of "agent of a foreign power" in FISA to include any non-U.S. person who "is reasonably expected to possess, control, transmit, or receive foreign intelligence information while such person is in the United States," if the government certifies that the foreign intelligence information is "significant."

1. Background on Current FISA's Basic Requirements.

To understand Section 401(a), it is necessary to review two aspects of FISA as it stands today. First, under current law, every FISA application for electronic surveillance or a physical search must include a statement of facts that is "relied upon by the applicant to justify his belief,"[3] and used by the FISC to determine probable cause, that the target of the surveillance or search is a "foreign power" or an "agent of a foreign power."[4] This is often referred to as the statute's probable-cause requirement.

Second, every FISA application today must also contain a certification, by a high-ranking executive branch official, that the information sought is "foreign intelligence information" and that a significant purpose of the search or surveillance is to obtain "foreign intelligence information" – a term that is defined to include information that is relevant or necessary to the ability of the United States to protect against various specified foreign threats to national security, including attack, sabotage, international terrorism, and espionage.[5] This is often referred to as the statute's purpose requirement.

Together, the probable-cause and purpose requirements are the fundamental limit on (and justification for) the use of FISA. They distinguish the statute from other information-gathering techniques used in other contexts, such as wiretapping in ordinary criminal investigations under Title III.[6]

2. FISA's Definition of "Agent of a Foreign Power."

Both "foreign power" and "agent of a foreign power" are defined in great detail in current Section 1801 of FISA.[7] Broadly speaking, a "foreign power" is an entity, such as a nation or an organization, including an international terrorist group,[8] and an "agent of a foreign power" is an individual who is in some way affiliated with a foreign power, such as a member of an international terrorist group.[9] Under current law, the only exception to that general rule of affiliation is the so-called "lone wolf" provision of FISA, which states that a non-U.S. person may be an "agent of a foreign power" if he "engages in international terrorism or activities in preparation therefor[]," regardless of whether he has a relationship with a terrorist group.[10] As I understand it from the government's public statements, the lone-wolf provision was designed to reach cases where (1) an individual genuinely is acting alone, perhaps inspired by, but not actively working for, an international terrorist group; or (2) the individual is indeed working for an international terrorist group, but the government cannot establish probable cause of that fact. In an era of widespread, ideologically-driven international terrorism, and proliferating nuclear weapons that fit inside carry-on luggage, this provision makes sense.

Section 401(a) of the government's proposal would expand on the rationale underlying the lone-wolf provision by creating what amounts to a catch-all provision for non-U.S. persons. Under this provision, if the government reasonably believes that the non-U.S. person has foreign intelligence information, the person is an agent of a foreign power and may be targeted. In other words, Section 401(a) effectively merges the statute's probable-cause and certification requirements.

3. FISA's Definition of "Foreign Intelligence Information."

Section 401(a) requires the "foreign intelligence information" sought under the catch-all provision to be "significant." I am not sure what that would mean. Current FISA contains five separate, but overlapping, definitions of "foreign intelligence information," divided into two sets. The first set defines "foreign intelligence information" in terms of protecting against various foreign threats to the national security.[11] This is sometimes referred to as protective foreign intelligence. The first set of definitions provides:

> Foreign intelligence information means –
>
> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –
>
> (A) actual of potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power[12]

The second set of definitions relates to the executive branch's need for affirmative foreign intelligence information to conduct foreign relations and make foreign policy decisions. This is sometimes referred to as affirmative foreign intelligence. This second set of definitions provides that foreign intelligence information also means –

> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.[13]

As these definitions make clear, apart from being divided into two sets – protective and affirmative intelligence – "foreign intelligence information" is also defined under two standards. Information "concerning a United States person" (e.g., a citizen or lawful permanent resident alien) may be foreign intelligence information only if it is "necessary" to the goal it serves (e.g., the ability of the United States to protect against international terrorism). By contrast, information concerning a non-U.S. person may be foreign intelligence information if it is merely "relevant" to that goal.

Congress imposed the "necessary" standard to protect the privacy of United States persons "from improper activities by [U.S.] intelligence agencies" while also protecting the United States and its allies "from hostile acts by foreign powers and their agents."[14]

"Necessary," according to the 1978 House Report, means that the information "is both important and required," not just that its collection would be "useful and convenient"; the government must show a "significant need" for the information.[15] Although the House Report acknowledges that the term "necessary" could encompass "every possible bit of information about a subject because it might provide an important piece of the larger picture," it explains that "such a reading is clearly not intended."[16]

The difference between "necessary" and "relevant" may prove elusive. For example, investigators may find it difficult to determine, especially at the early stages of an investigation, whether information concerning a U.S. person is actually necessary to protect against terrorism or instead merely "relates to" that goal. The House Report itself reflects this problem of interpretation. Although the Report disapproves a broad view of "foreign intelligence information" that would encompass information "about a U.S. person's private affairs," the Report suggests that such information constitutes foreign intelligence information if "it *may* relate to his activities on behalf of a foreign power."[17] As a practical matter, moreover, personal information about spies and terrorists is nearly always arguably "necessary" to the protection of national security, because knowledge of the movements, habits, and preferences of these individuals may be crucial in thwarting threats to the national security.[18]

By referring to "significant" foreign intelligence information, does Section 401(a) mean to apply the U.S.-person standard – "necessary" – to information that, in most cases, will be "concerning" a non-U.S. person and therefore otherwise subject to the "relevant" standard?[19] I don't know. The "significant" adjective seems to reflect the government's sense that this provision should not be used except in important cases. It may be better, however, to express that sense through the existing syntax of FISA's definition of foreign intelligence information. It also may be wise explicitly to limit the use of this provision to cases where the government affirms that it cannot satisfy the other definitions of "agent of a foreign power" in FISA.

Section 401(b)

Section 401(b) of the government's proposal would amend FISA's definition of "electronic surveillance." This would be a very significant change in the law. It should be the hard center of any attention that is paid to this proposal. Unfortunately, to understand the government's proposal, it is necessary first to understand current law, and current law is enormously complex. In the discussion that follows, I try to explain the importance of the definition of "electronic surveillance" to the regulatory scheme established by FISA (part 1); provide an overview (part 2), a detailed analysis (part 3), and a description of the limits (part 4) of the current definition of "electronic surveillance; explain the definition of "physical search" in current FISA, because it intersects directly with the definition of "electronic surveillance" (part 5); and explain how the definitions apply to various forms of real-world surveillance (part 6). I then try to do the same for the government's proposed new definition of "electronic surveillance" (part 7), and discuss how the proposed definition may intersect with Title III (part 8).

1. Background on the Significance of "Electronic Surveillance" as Defined by FISA.

FISA authorizes and regulates "electronic surveillance" by the government in certain circumstances, and the scope of the authorization and regulation depends largely on the meaning of that term. For example, the FISC has jurisdiction to hear applications for and grant orders approving "electronic surveillance" anywhere within the United States under the procedures set forth in FISA.[20] Those procedures generally require the government to submit an application for an order approving "electronic surveillance,"[21] and authorize a judge of the FISC to enter an *ex parte* order approving the "electronic surveillance" if the application meets the statutory requirements.[22] The President, through the Attorney General, may authorize "electronic surveillance" without a court order under certain circumstances.[23] FISA also regulates the use of information obtained or derived from "electronic surveillance,"[24] requires certain reporting to Congress and public disclosure concerning "electronic surveillance,"[25] and provides civil and criminal penalties for anyone who engages in "electronic surveillance" under color of law except as authorized by statute.[26] **In short, the entire framework of subchapter I of FISA[27] turns on the meaning of "electronic surveillance."**

2. Overview of FISA's Current Definition of "Electronic Surveillance."

The current definition of "electronic surveillance" in FISA contains four separate subsections, and is enormously complex.[28] I therefore begin with an overview of each of the four subsections of the definition, discussing briefly the basic kinds of communications and surveillances to which each subsection applies. This is meant to serve as an orientation for the more technical discussion that follows.

The first subsection of the current definition of "electronic surveillance," 50 U.S.C. § 1801(f)(1), defines the term to mean:

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

This is the principal provision applicable to wiretaps of United States persons – e.g., U.S. citizens or permanent resident aliens – who are inside the United States. In essence, it provides that the government must obey FISA (e.g., by obtaining a FISC order) whenever it tries to overhear or record a telephone call or other similar communication from such a person, if (and only if) a warrant would be necessary for the same wiretap conducted for ordinary law enforcement purposes under Title III[29] or a similar provision. The subsection applies equally to domestic and international communications made by U.S. persons in the United States.

The second subsection of the definition, 50 U.S.C. § 1801(f)(2), defines "electronic surveillance" to mean:

> the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18, United States Code.

This provision applies to wire communications, such as corded telephone calls while they are traveling on a wire or cable, regardless of the citizenship or immigration status of the persons involved, as long as either the sender or recipient of the communication is in the United States, and neither sender nor recipient consents to the wiretap. This provision is broader than the first subsection of the definition in that it applies to non-U.S. persons, such as visiting foreigners, but it is narrower in that it applies only to wire communications, not to radio communications. It also excludes a narrow band of communications of computer trespassers, who are likewise unprotected by Title III.

The third subsection of the definition, 50 U.S.C. § 1801(f)(3), defines "electronic surveillance" to mean:

> the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States.

This provision applies only to radio communications, such as CB or ham radio signals, or the signals emitted by a cordless or cellular telephone. Like the first subsection, it applies only when a law-enforcement warrant would otherwise be required for the surveillance. It also applies only when all intended parties to the radio communication are located in the United States, meaning that it does not reach international radio communications.

Finally, the fourth subsection of the definition, 50 U.S.C. § 1801(f)(4), defines "electronic surveillance" to mean:

> the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

This part of the definition applies principally to microphone surveillance rather than to traditional wiretapping. If the government installs a hidden microphone anywhere in the United States, and acquires an oral communication (rather than a telephone call), it may be governed by this provision. The same is true of video surveillance.

3. Detailed Analysis of FISA's Current Definition of "Electronic Surveillance".

A real understanding of the definition of "electronic surveillance" requires more analysis than the casual overview above. The definition, including the relationships among its four subsections, ultimately turns on six separate factors. These are the factors that must be considered when determining whether any particular act of surveillance is "electronic surveillance" as defined by FISA today.

(1) the type of information being acquired (wire communication, radio communication, or other information);

(2) the type of acquisition (e.g., through the use of a surveillance device or the installation of such a device, intentional or otherwise);

(3) the location where the acquisition occurs (inside or outside the United States);

(4) the status of the targets of the surveillance (as U.S. persons or non-U.S. persons);

(5) the location of the targets (inside or outside the United States); and

(6) the existence (or not) of a reasonable expectation of privacy and the need (or not) for a warrant to engage in the surveillance under law-enforcement rules.

In this part of my comments, I discuss each of these six factors in detail, explaining where and how each applies to the four subsections of the definition. I end this part with a summary chart describing the definition of "electronic surveillance" in terms of the six factors.

a. Type of Information or Communication.

There are three kinds of information subject to "electronic surveillance" under current FISA: wire communications,[30] radio communications,[31] and information that is neither a wire nor a radio communication.[32] FISA does not define the term "communication," but the dictionary defines it as an expression or exchange of information or ideas.[33] As such, it includes all of the following: an oral conversation, a sign-language conversation, a letter, a telegram, a telephone call, an electronic mail message, or any other form of communication that advancing technology permits.[34]

A "communication" as the term is used in FISA's definition of electronic surveillance must have a "sender" and one or more "recipients."[35] Although the statute does not make clear whether the sender and recipient of a communication can be the same person – e.g., when a person sends an e-mail from his work e-mail account to his personal e-mail account – nothing in the text or legislative history of FISA overtly conflicts with treating the same person as both sender and recipient of a communication. Similar issues may arise with respect to diaries, task lists, oral statements of persons who talk to themselves, and certain kinds of arguably "symbolic" speech.[36]

i. Wire Communication.

Two of the four parts of the current definition of "electronic surveillance" – Subsections (1) and (2) – apply to "wire communications." FISA defines "wire communication" as "any communication while it is being carried by a wire, cable, or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications."[37] In keeping with the plain language of the definition, FISA's legislative history explains that communications are "wire communications" only "while they are being carried by a wire."[38] Thus, a cordless telephone call is not a wire communication while the signal travels from the handset to the base station (it is, instead, a radio communication), although the call would become a wire communication once it arrives at the base station and begins moving over a telephone line. The same logic applies to mobile telephone signals while they travel between a mobile handset and a telecommunication provider's tower; they would begin as radio communications between the handset and the tower, and would become wire communications after they arrived at the tower.[39] An e-mail message is a "wire communication" while transiting over a wire or cable, but not while transiting as a radio signal to or from a BlackBerry or other wireless e-mail device.

These distinctions can affect where and how the government may acquire a communication under current law. For example, monitoring a cordless or mobile telephone call between the handset and the base station or tower is not electronic surveillance under Subsection (2), because that provision applies only to "wire communications." As discussed below, however, it may be electronic surveillance under Subsections (1) or (3), because those provisions apply to "radio communications." Conversely, monitoring the same telephone call by tapping the telephone wires could be electronic surveillance under Subsections (1) or (2), but could not be electronic surveillance under Subsection (3), because Subsection (3) does not apply to wire communications.[40]

By restricting a "wire communication" to communications while being carried by wire, current FISA contrasts with Title III, which defines "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce."[41] As Congress understood when it enacted FISA, Title III's definition applies to a (wire) communication at all stages of transmission if the communication travels "in whole or in part" by wire on its journey from "the point of origin" to "the point of reception."[42]

Not all wires carry "wire communications" as defined in current FISA. Rather, the wire must be "furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications."[43] The common carrier must be in the business of providing interstate or international service (though of course the particular communication in question may be wholly intrastate[44]), and it must be "a U.S. common carrier and not a foreign common carrier."[45]

FISA does not define "common carrier," but the dictionary definition of the term is a "commercial enterprise that holds itself out to the public as offering to transport freight or passengers for a fee."[46] In the context of communications, rather than transportation, Title III cross-references and incorporates the federal Communications Act's definition of the term, which includes "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy, ... but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier."[47]

In part because of the cross-reference in Title III, courts might interpret current FISA's use of the term "common carrier" in accord with the Communications Act,[48] although the two statutes have very different purposes, and doing so could introduce substantial uncertainty and complexity into FISA's statutory scheme.[49] A traditional local or long-distance telephone company is the paradigmatic example of a "common carrier" under the Communications Act.[50] A mobile telephone company is also a common carrier under the Communications Act.[51] A cable television operator is not a "common carrier" under the Communications Act,[52] except insofar as it offers circuit-switched telephone service.[53] The Supreme Court has upheld the FCC's determination that "cable companies that sell broadband Internet service do not provide 'telecommunications servic[e]' as the Communications Act defines that term, and hence are exempt from mandatory common-carrier regulation."[54] Thus, if current FISA's reference to "common carrier" were interpreted in accord with the Communications Act, information (such as e-mail) being carried on a cable owned and offered by a cable modem service provider would not be a "wire communication" under FISA, and acquisition of such information would not be "electronic surveillance" under Subsections (1) and (2) of the definition. An ISP also is not a "common carrier" under the Communications Act, [55] but the telephone lines used to connect dial-up users to an ISP are usually provided by a telephone company or other common carrier.[56]

ii. Radio Communication.

Current FISA does not define the term "radio communication." As a scientific matter, radio signals are defined by their wavelength on the electromagnetic spectrum.[57] A classic example of a radio communication would be a Citizens' Band (CB) or Bluetooth signal.[58] But Congress apparently meant "radio communication" in FISA to include microwaves,[59] which may be distinguished technically from radio waves (because they have a shorter wavelength).[60] Indeed, Congress may have intended to cover the entire electromagnetic spectrum of wireless communications. The question is not authoritatively settled in publicly-available materials. Like a wire communication, however, a radio communication presumably would be a radio communication only so long as it is being carried by radio – i.e., not when the communication has left the radio waves and is transiting by wire, and not after it reaches its destination at the recipient.

iii. Information Other than Wire or Radio Communications.

The final definition of "electronic surveillance," in current Subsection (4), applies only to information acquired from sources other than wire and radio communications. This includes communications that are not carried by wire or radio, such as oral communications (acquired by

hidden microphone). It also includes non-communicative information – for example, the objects in a room, or images of a terrorist planting explosives (acquired by video cameras) – and the use of transponder devices attached to a vehicle or other object that reveal the object's location.[61]

b. Type of Acquisition.

Surveillance is "electronic surveillance" under current FISA only when the government "acquires" information.[62] FISA does not define that term, but its ordinary meaning – to gain possession of – includes not only recording and listening to a communication, but also listening to the communication without recording it, and (probably) recording it without listening to it. At least one court has held that "acquisition" as used in Title III[63] includes recording the contents of a conversation even if the recording is never listened to.[64] The same reasoning and result probably should apply to FISA recordings made and not reviewed, even if (as sometimes happens), the recordings are in fact erased without ever being heard.[65]

On the other hand, the government has in the past argued successfully under Title III (and, it appears, FISA) that the Carnivore (DCS-1000) system does not "intercept" all of the communications that pass into its programming filters.[66] Carnivore is a device that captures specified packets of data from a packet-switched computer network. To do this, Carnivore instantaneously copies into its random access memory all packets of data that are transiting the network, and then copies some of those packets to permanent memory according to its programming instructions (e.g., all packets going to a particular e-mail address on the network). The gist of the government's argument is that no interception or acquisition occurs "during all the [initial] filtering/processing" stage in which Carnivore selects the desired from the undesired packets on the monitored network, because "no FBI personnel are seeing any information – all of the information filtering/processing, and purely in a machine-readable format, is occurring exclusively 'within the box.'"[67] There may well be a reasonable distinction between the instantaneous, ephemeral "recording" of disintegrated communications in short-term electronic computer memory, and the permanent recording of integrated communications on tape or other permanent media. Essentially, the argument would be that that if the government has intercepted or otherwise enjoys meaningful access to information (including a communication), it has "acquired" that information.[68]

Acquisition is "electronic surveillance" under all four parts of the current definition only when it involves the use of an "electronic, mechanical, or other surveillance device."[69] FISA does not define that term. Title III provides that the term "electronic, mechanical, or other device" means "any device or apparatus which can be used to intercept a wire, oral, or electronic communication," but does not include the following:

> (a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic

communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

(b) a hearing aid or similar device being used to correct subnormal hearing to not better than normal.[70]

The exceptions in Title III's definition – for certain telephone equipment furnished to subscribers – are more significant in that statute than in FISA because Title III generally forbids (and prescribes penalties for) interception of communications by any party, and then provides exceptions to that general prohibition for authorized surveillance by the government.[71] By contrast, FISA authorizes and regulates certain investigative activity by the government; it prescribes civil and criminal penalties only for illegal electronic surveillance conducted "under color of law."[72]

FISA's legislative history states that the use of the phrase "surveillance device" does not encompass "lock picks, still cameras, and similar devices," even though they "can be used to acquire information, or to assist in the acquisition of information."[73] By analogy to Title III's exemption for hearing aids, ordinary eyeglasses also would not be a FISA "surveillance device." The same is probably also true of "[b]inoculars, dogs that track and sniff out contraband, searchlights, fluorescent powders, automobiles and airplanes,"[74] but somewhere on the continuum between ordinary eyeglasses and sophisticated thermal imagers, items used to aid surveillance become "surveillance devices" under FISA.[75] As a practical matter, the more esoteric the technology, the more likely courts probably would be to find it a "surveillance device."[76]

There have been a number of decisions on the meaning of "surveillance device" as used in the provision of Title III making it illegal to use or possess such devices when they are designed primarily for surreptitious surveillance[77] (with many of the decisions involving cable television descramblers[78]), but these decisions often turn on the defendant's knowledge of whether the device's design makes it primarily suitable for surreptitious surveillance, and are therefore not a completely reliable guide to the meaning of "surveillance device" in FISA.[79] To be sure, the government may use its share of microphones disguised as martini olives,[80] but its authority to compel the assistance of third parties (e.g., landlords and telephone companies) means that its FISA surveillance devices need not always be designed primarily for surreptitious use.

To qualify as "electronic surveillance" under the first three subsections of FISA's current definition, a surveillance device must be used to acquire the "contents" of a communication. When used with respect to a communication, FISA defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication."[81] This definition differs from Title III's definition of "contents"[82] because it includes information concerning the "existence" of a communication and the "identity of the parties" to it.[83] Thus, it effectively covers any information about a communication, including the sort of routing and addressing information (e.g., telephone numbers) acquired by pen/trap surveillance.[84] Subsection (4) is even broader, and applies to any "information" acquired, even if it is not a communication.

c. Location of Acquisition.

Two parts of FISA's current definition of "electronic surveillance," Subsections (2) and (4), apply only when the surveillance – the acquisition of the contents of the communication or the use of the surveillance device – occur inside the United States.[85] Under a separate provision of FISA, "'United States,' when used in a geographic sense, means all areas under the territorial sovereignty of the United States and the Trust Territory of the Pacific Islands."[86] This definition could arguably include the U.S. Naval Base in Guantanamo Bay, Cuba,[87] although the 1978 House Report on FISA states that U.S. military bases located abroad are *not* part of the "United States" when used in a geographic sense.[88] Surveillance may be "electronic surveillance" under Subsections (1) and (3) regardless of where it occurs.

d. Targets.

Under Subsection (1) of the current definition, acquisition of the contents of a wire or radio communication (using a surveillance device) is "electronic snrveillance" only if the communication is "sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person." This provision may apply not only to FISA applications that identify a U.S. person as a target, but also to so-called "watchlisting," a process that involves monitoring a communications channel and using automated systems to intercept particular communications for review. Based on affidavits from the NSA, the D.C. Circuit has described watchlisting as follows:

> **NSA monitors radio channels. Because of the large number of available circuits, however, the agency attempts to select for monitoring only those which can be expected to yield the highest proportion of foreign intelligence communications. When the NSA selects a particular channel for monitoring, it picks up all communications carried over that link. As a result, the agency inevitably intercepts some personal communications. After intercepting a series of communications, NSA processes them to reject materials not of foreign intelligence interest. One way in which the agency isolates materials of interest is by the use of [l]ists of words and phrases, including the names of individuals and groups .... These lists are referred to as "watch lists" by NSA and the agencies requesting intelligence information from them.[89]**

In essence, watchlisting resembles a sophisticated version of using search terms to query a large database of acquired information, as is now common in pre-litigation discovery, or in legal research using Westlaw or its equivalents.[90] Under FISA, the argument would be that this kind of watchlisting – or any deliberate use of a surveillance device to monitor a specific communications channel where the but-for purpose of the surveillance is to acquire communications from a U.S. person in the U.S. – is "targeted" surveillance under Subsection (1). The only exception identified in the legislative history is where a U.S. person's communication is "acquired unintentionally."[91]

The remaining parts of the current definition – Subsections (2)-(4) – do not require targeted surveillance. In practice, of course, all FISC-authorized electronic surveillance has a "target," but the definitions mean that the government must adhere to FISA – including the requirement to designate a target and establish that it is a foreign power or an agent of a foreign power – when it conducts "electronic surveillance," even if (the government would argue) there is in fact no target, or if the target is not a U.S. person. Put another way, FISA provides that the government cannot engage in broad-brush, non-targeted surveillance as defined by Subsections (2)-(4) unless it can in fact identify a "target" and satisfy the statute's other requirements.

e. Location of Targets.

Certain parts of the current definition of "electronic surveillance" apply only where a communication's sender, recipient, or both are located in the United States. Under Subsection (1), the target of the surveillance (who may be either a sender or recipient of a communication) must be located in the United States, and under Subsection (2) either the sender or a recipient must be located in the United States. Under Subsection (3), both sender and all intended recipients must be in the United States. Under Subsection (4), the location of sender and recipient is irrelevant, but the surveillance device must be used in the United States. As discussed above, FISA defines "United States" when used in a geographic sense to include all territory under U.S. sovereignty.[92] As discussed below, difficult issues can arise when surveillance targets communications that can be sent or received from multiple locations, such as a mobile telephone call or electronic mail.

f. Reasonable Expectation of Privacy and Warrant Required for Law Enforcement.

Three of the four parts of FISA's current definition of "electronic surveillance" – Subsections (1), (3), and (4) – apply only when "a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[93] The first part of this standard – "reasonable expectation of privacy" – is a term of art from U.S. Constitutional law. It debuted in the Supreme Court in Justice Harlan's concurring opinion in *Katz v. United States*,[94] a decision holding that electronic surveillance of a telephone call is a Fourth Amendment "search." The phrase now serves as a talisman for situations in which the Fourth Amendment applies.[95]

The language of current FISA and its legislative history suggest that the reasonable expectation of privacy does not depend on the status of the individual whose privacy is being invaded by the surveillance. While Congress was considering FISA, the Department of Justice's Office of Legal Counsel "opined that foreign governments – and in some circumstances their diplomatic agents [–] have no fourth amendment rights under the Constitution."[96] The Supreme Court has stated that it is an open question "whether the protections of the Fourth Amendment extend to illegal aliens in this country."[97] Congress made clear in the legislative history that FISA's definition of "electronic surveillance" does not turn on that question. Instead, the definition depends on "the reasonableness of the expectation of privacy that a U.S. person would have with respect to [the surveillance] activity," and "is intended to exclude only those surveillances which would not require a warrant even if a U.S. citizen is a target."[98]

Although the legislative history refers to the FISA "target," the "reasonable expectation of privacy" in question should include expectations held by persons other than the FISA target or the parties to the intercepted communication (or their U.S. citizen equivalents). That follows from the statute's use of the phrase "circumstances in which *a* person" has a reasonable expectation of privacy,[99] a standard that includes any person.[100] The broader reading also makes sense in the context of FISA's physical search provisions, where the identical phrase is used.[101] If the only relevant expectation of privacy were the target's, then the FISC would have no jurisdiction[102] to authorize the physical search of a third party's home for information concerning a FISA target who was, for example, a business invitee in that home.[103]

The second part of the standard – "a warrant would be required for law enforcement purposes" – establishes a related, but different test. It is not merely an empirical test: the legislative history makes clear that "a warrant would be required for law enforcement purposes" does "not mean that a court must previously have required a warrant for the particular type of surveillance activity carried out."[104] As Congress properly understood, the executive branch may decide not to use its most effective classified intelligence collection methods in criminal cases. As a result, the surveillance "techniques involved [in FISA surveillance] may not have come before a court for a determination as to whether a warrant is required."[105] In such a situation, FISA's legislative history explains, the government should make "an assessment of the similarity with other surveillance activities which the courts have ruled upon."[106] Where an intelligence agency "wishes to use a new surveillance technique," the legislative history states that it should "seek a ruling from the Attorney General as to whether the technique requires a court order."[107] Similarly, FISC Rule 10(a)(i) provides that where the government requests "authorization to use a new surveillance or search technique," it must "submit a memorandum to the Court which: (A) explains the technique; (B) describes the circumstances of the likely use of the technique; (C) discusses legal issues apparently raised by the technique; and (D) describes proposed minimization procedures to be applied to the use of the technique."[108]

Surveillance is "electronic surveillance" under current Subsections (1), (3), and (4) only when both conditions are met – that is, only when there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[109] There are situations in which a reasonable expectation of privacy exists, but no warrant is required – for example, a search (including electronic monitoring) pursuant to consent,[110] a search incident to arrest,[111] the search of a car,[112] and an inventory search.[113] Conversely, as discussed in more detail below, there are situations in which a warrant is clearly required but there may be no reasonable expectation of privacy (at least as held by the target of the surveillance or search),[114] and other situations in which there is clearly no reasonable expectation of privacy but a warrant may be required.[115]

In the USA PATRIOT Act,[116] Congress carved out surveillance of computer trespassers from the definition of "electronic surveillance" in current Subsection (2) by cross-referencing a provision of Title III, 18 U.S.C. § 2511(2)(i).[117] Under that provision of Title III, the government may conduct surveillance of a hacker's wire or electronic communications[118] on a computer, with the consent of the computer's owner, if those communications are relevant to a lawful investigation and the surveillance acquires only communications to or from the hacker. This provision may not be necessary in most situations: if a trespasser's transmission of electronic hacking tools to a victim's protected computer is a "wire communication" under FISA,

as it must be to fall within Subsection (2), then the victim will usually (but perhaps not always[119]) be a "party thereto," whose consent removes the surveillance from Subsection (2) regardless of Section 2511(2)(i). Subsection (2) is, however, the only part of FISA's definition of "electronic surveillance" that does not explicitly state that "a warrant would be required for law enforcement purposes," and so the cross-reference may be understandable as an act of caution in a difficult statutory matrix.

g. **Chart.**

The following chart presents the four subsections of FISA's current definition of "electronic surveillance" in terms of the six factors discussed above.

Statute	50 U.S.C. § 1801(f)(1)	50 U.S.C. § 1801(f)(2)	50 U.S.C. § 1801(f)(3)	50 U.S.C. § 1801(f)(4)
Type of communication	Wire or radio	Wire	Radio	Non-wire, non-radio
Type of Acquisition	Acquisition of contents by electronic, mechanical, or other surveillance device	Acquisition of contents by electronic, mechanical, or other surveillance device	Intentional acquisition of contents by electronic, mechanical, or other surveillance device	Installation or use of electronic, mechanical, or other surveillance device for monitoring to acquire information
Location of Acquisition	No geographical limit on acquisition	Acquisition must occur in the U.S.	No geographical limit on acquisition	Device must be used in the U.S.
Targets	Sent by or intended to be received by a particular, known U.S. person who is intentionally targeted	To or from a person	No limit on persons (all persons)	No limit on persons (all persons)
Location of Targets	Targeted U.S. person must be in the U.S.	Communication must be to or from a person in the U.S.	Sender and all intended recipients must be located in the U.S.	No limit on location of persons (all places)
Reasonable Expectation of Privacy (REP) and Warrant Required for Law Enforcement (LE) Purposes	A person has a REP and warrant required for LE purposes	Without consent of any party to the communication, not including trespassers as defined in 18 U.S.C. § 2511(2)(i)	A person has a REP and warrant required for LE purposes	A person has a REP and warrant required for LE purposes

4. **Limits in FISA's Current Definition of "Electronic Surveillance."**

It may be helpful to review the limits in the current definition of "electronic surveillance" – i.e., surveillance activity that is not "electronic surveillance" under current FISA, and therefore is not regulated by FISA today. There are four important limits.

First, the statute does not apply where all parties to a communication are located abroad. Purely foreign communications are simply beyond FISA's ambit.[120] That is the case regardless of the type of communication (wire or oral), the type of acquisition, the location of acquisition (inside or outside the U.S.), the parties' status as U.S. persons or targets, and any person's expectation of privacy. That is because Subsections (1)-(3) of the definition each require at least one party to a communication to be located in the United States,[121] and Subsection (4) does not apply outside the U.S.[122]

Second, FISA does not apply where the target is located abroad, and the surveillance (acquisition) occurs abroad, regardless of any other statutory factor.[123] Where the target is abroad, Subsections (1) and (3) do not apply; and where the acquisition occurs abroad, Subsections (2) and (4) do not apply. Surveillance conducted abroad, targeting U.S. persons located abroad, is regulated under Section 2.5 of Executive Order 12333 and the Fourth Amendment. As FISA's legislative history explains, the statute "does not afford protections to U.S. persons who are abroad," and "does not bring the overseas surveillance activities of the U.S. intelligence community within its purview."[124]

Third, FISA does not apply to wire surveillance not targeting a U.S. person if the surveillance (acquisition) occurs abroad, regardless of any other statutory factor. This kind of surveillance may intercept wire communications to or from U.S. persons in the United States – e.g., if a U.S. person calls (or is called by) a surveillance target located abroad whose calls are being acquired abroad. Again, however, a U.S. person located in the U.S. cannot be the *target* of the surveillance without triggering Subsection (1), even if the surveillance (acquisition) occurs abroad.

Fourth and finally, FISA does not apply to radio surveillance not targeting a U.S. person where any party to the radio communication is outside the United States, regardless of any other statutory factor. It may be that some radio communications cannot be the subject of "electronic surveillance" because, to the extent that they are omni-directional signals easily intercepted by the general public, they do not generate a reasonable expectation of privacy.[125] To the extent that there is a reasonable expectation of privacy in a radio communication – e.g., due to encryption – however, the government may intentionally acquire the communication without a FISC order if the target is not a U.S. person and either the sender or any intended recipient is outside the United States.[126]

5. FISA's Current Definition of "Physical Search".

To understand the current definition of "electronic surveillance," it is also necessary to understand the current definition of "physical search." The definition of "physical search" functions in subchapter II of current FISA as the definition of "electronic surveillance" functions in subchapter I. It determines the FISC's jurisdiction,[127] the goal of a FISA application[128] and the subject-matter of an authorization order,[129] the scope of the President's power under FISA to act without FISC approval,[130] the scope of the limits on use of information derived from FISA,[131] the subject-matter of congressional reporting and oversight,[132] and the applicability of civil and criminal penalties for improper conduct.[133]

Fortunately, current FISA's definition of "physical search" is simpler than its definition of "electronic surveillance." Under 50 U.S.C § 1821(5), the term "physical search" means:

> [1] any physical intrusion within the United States[134] into premises or property (including examination of the interior of property by technical means) [2] that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, [3] under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but [4] does not include (A) "electronic surveillance", as defined in section 1801(f) of this title, or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 1801(f) of this title.

Taking this definition one phrase at a time, a "physical intrusion … into premises or property (including examination of the interior of property by technical means)" means physically entering a place protected by a reasonable expectation of privacy, or using technology to gain information about the interior of the place that would normally require a physical intrusion. Its meaning is illustrated by a 2001 Supreme Court decision, *Kyllo v. United States*.[135] In *Kyllo*, a federal agent in a car parked across the street from a private home used a "thermal imager" to scan and detect unusual heat patterns emanating from the home.[136] Based in part on those heat patterns, the agent "concluded that [Kyllo] was using halide lights to grow marijuana in his house, which indeed he was."[137]

The Supreme Court held that the thermal scan was a Fourth Amendment "search" requiring a warrant. It explained that until "well into the 20th century," Fourth Amendment jurisprudence "was tied to common-law trespass,"[138] which meant that while physical intrusion required legal justification, ordinary visual surveillance from a public place did not, because "the eye cannot by the laws of England be guilty of a trespass."[139] The issue for the Court in Kyllo was "how much technological enhancement of ordinary perception from such a [public] vantage point, if any, is too much."[140] The answer, according to the Court, was as follows: "obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search – at least where (as here) the technology in question is not in general public use."[141] That appears to be the standard applicable to the phrase "examination of the interior of property by technical means" in FISA's definition of "physical search," although the matter is not clearly settled.

The second phrase in the definition – "seizure, reproduction, inspection, or alteration of information, material, or property" – also has a fairly settled meaning. The Supreme Court explained in *Kyllo* that the dictionary definition of "search" included to "look over or through for the purpose of finding something; to explore; to examine by inspection; as, to search the house for a book; to search the wood for a thief."[142] The Court has repeatedly held that a "'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[143] FISA's legislative history explains that the word "alteration" is

included in the definition to "ensure that the [FISC] is informed and approves of any planned physical alteration of property incidental to a search, e.g., the replacement of a lock so as to conceal the fact of the search."[144] The third phrase in the definition – "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" – has the same meaning as its counterparts in the definition of "electronic surveillance," as discussed above.

The two exclusions in the current definition of "physical search" are important to the orderly functioning of FISA as a whole. The first exclusion – denoted [4](A) in the block quote above – simply means that the same conduct cannot be both electronic surveillance and a physical search; it must be one, or the other, or neither. The absence of a corresponding exclusion in the definition of "electronic surveillance" probably means that it yields only when it does not apply. Thus, where the same actions may be characterized as both electronic surveillance and as a physical search, they should be treated as surveillance. On that approach, use of the thermal imager in *Kyllo* should be "electronic surveillance" under Subsection (4),[145] because the imager is a "surveillance device" that was used "for monitoring to acquire information," even though the thermal scan could also be characterized as an "examination of the interior of property by technical means."

The second exclusion has the same function for certain foreign intelligence surveillance that is not "electronic surveillance" as defined by current FISA, and mirrors an exclusion in Title III.[146] As the 1978 legislative history of FISA explains, "the legislation does not deal with certain international signals intelligence activities currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."[147]

6. Application of FISA's Current Definitions.

As the foregoing discussion reveals, FISA's current definitions of "electronic surveillance" and "physical search" are very complex. Set out below are several hypothetical examples that may help illustrate the meaning of the definitions as applied to particular facts or scenarios.

a. Traditional Land-Line Telephone Calls.

It is "electronic surveillance" under current Subsection (1) if the government uses a surveillance device to acquire the contents of a cordless or corded land-line telephone call between a U.S. person in one state, Mr. *A*, and another person of any nationality in another state, Ms. *B* (it does not matter who called whom), without the consent of *A* or *B*, as part of surveillance targeting *A*. That is because a telephone call is either a "wire communication" (when intercepted from a wire) or a "radio communication" (when intercepted from the air); recording the call acquires its contents; the device used to record the call will be a "surveillance device"; *A* is the intentional target of the surveillance; *A* is a U.S. person; *A* is in the United States; there is a reasonable expectation of privacy in a telephone call;[148] and a Title III warrant would be required to conduct surveillance of the call for law enforcement purposes.[149]

The same is true if *B* is located abroad instead of in the United States, or if both *A* and *B* are in the same state (as long as they are using an interstate telephone company's facilities), regardless of where the surveillance occurs. As FISA's legislative history explains, Subsection (1) "protects U.S. persons who are located in the United States from being targeted in their domestic or international communications without a court order no matter where the surveillance is being carried out."[150]

If *A* (the target) is *not* a U.S. person, surveillance of the telephone call between *A* and *B* is not "electronic surveillance" under current Subsection (1). It is, however, "electronic surveillance" under current Subsection (2) if the contents of the call are acquired from a wire (not a radio signal), whether or not the government is targeting either *A* or *B* (or anyone else), as long as at least one of them is in the United States, the acquisition of contents occurs in the United States, and neither *A* nor *B* consents. Thus, again assuming that *A* is not a U.S. person, it is not "electronic surveillance" to acquire the contents of a call between *A* and *B* if both *A* and *B* are outside the United States, if the acquisition occurs outside the United States, or if one of them consents.[151]

If the contents of the call between *A* and *B* are intentionally acquired from a radio signal (not a wire), then the surveillance is "electronic surveillance" under current Subsection (3) if both *A* and *B* are located in the United States, regardless of where the surveillance occurs. Radio surveillance where *A* is not a U.S. person is not "electronic surveillance" if either *A* or *B* are outside the United States. Thus, if the government intercepts the radio portion of a cordless international call from a non-U.S. person in the United States, it probably is not electronic surveillance.[152]

b. Faxes.

Fax communications that transit conventional telephone lines should generally be indistinguishable from spoken telephone conversations under current FISA. Although a fax message is not an aural communication, like a telephone call, it is a "wire communication" under FISA while it is being carried on a wire, even though it would not be a "wire communication" under Title III.[153] A wireless fax machine would be treated like a cordless telephone, except that – because a fax is not aural and therefore may not be as easily intercepted – it would be even more likely than a cordless telephone call to generate a reasonable expectation of privacy.[154]

c. Mobile Telephone Calls.

Mobile telephones obviously raise geographical issues. When the government conducts surveillance of traditional land-line telephones (or fax machines), it knows where the telephone is located – that is the distinguishing feature of a land line. Thus, when the government monitors *A* talking (or faxing) on his home telephone, it can be reasonably confident that he is in fact at his home address. If *A* is a U.S. person, the government can therefore know, in advance, that the surveillance targeting him will be subject to current Subsection (1).

When *A* is using a mobile telephone, however, he may be virtually anywhere, including outside the United States.[155] When the government applies for a FISA order on A's mobile

telephone, it cannot know, in advance, whether or not he will use it to make calls from within the United States. Caution dictates obtaining a FISA order, of course, unless the government can be sure that *A* is in fact out of the country, but to the extent that *A* takes a temporary trip abroad, surveillance of calls made from his mobile phone may not be "electronic surveillance" under FISA.[156]

d. Microphones and Video.

If the government has a microphone concealed where *A* or *B* is located when making a private call (using any kind of telephone or other device), and the microphone acquires at least one side of the conversation, it is electronic surveillance under current Subsection (4) if the microphone is located in the United States. That is the case whether or not *A* and *B* are U.S. persons, and regardless of where *A* and *B* are located. The same holds true for microphone or video surveillance of *A* or *B* if they are engaged in an oral communication or even if they are not engaged in a conversation; "electronic surveillance" under current Subsection (4) applies to the acquisition of "information," not merely "communications."

e. E-Mail and Voice Mail Messages.

Electronic mail and voice mail messages raise difficult practical and legal issues under current FISA. The discussion begins with some background on how e-mail and voice mail function, and then considers the resulting legal implications under FISA.

i. Background on E-Mail and Voice Mail.

For purposes of the legal discussion that follows, here is a concrete (and somewhat oversimplified) description of how modern e-mail functions. The sender of an e-mail message writes the e-mail on his personal computer, which may be located virtually anywhere, using a software program like Microsoft Outlook or Eudora or AOL mail. He then hits the "send" button in that program, which transmits the e-mail message from his computer to his ISP. The e-mail is disintegrated into several discrete "packets" which are transmitted individually over the Internet – each packet may travel a different route from the others – until they converge at the recipient's ISP, where they are reintegrated into a coherent message that is stored on a server until the recipient logs in and reads the e-mail on his personal computer. Depending on whether the sender or recipient deletes the e-mail, and on their ISPs' own policies, the e-mail may remain in storage for some time after it has been read.[157]

Voice mail is similar in certain of those respects to e-mail: the caller telephones the recipient, and when no one answers, leaves a recorded message on the telephone company's electronic storage facilities. The recipient hears the recording when he dials in to those facilities to check his voice mail. Again, the voice mail is in storage with the telephone company at least until the recipient listens to it.

The foregoing descriptions reveal three important implications for the legal treatment of e-mail and voice mail under FISA. First, like mobile telephone calls, e-mails

and voice mails generate geographic issues: if *A* has an e-mail account with an ISP, he can access that account, and read his e-mail, from virtually anywhere in the world, including outside the United States. Again, therefore, the government cannot be sure that *A* will be in the United States when he sends or receives an e-mail. The same is true with respect to voice mail, which can also be accessed remotely.

Second, e-mail messages can be acquired after the fact from electronic storage in the sender's or recipient's e-mail accounts.[158] Unlike a plain old telephone service (POTS[159]) call, which involves a voice transmission over a dedicated circuit, e-mail messages are sent in the form of multiple packets that may travel over multiple electronic pathways from the sender to the recipient before being reassembled and stored for retrieval by the recipient. (This is the basic difference between a circuit-switched and packet-switched network.) Thus, unlike a telephone call, e-mail messages endure even after they have been sent, at a time when they are no longer "being carried" by a wire or radio wave.[160]

Third, e-mail and voice mail messages are communications entrusted to, and stored by, third parties, such as an ISP.[161] This raises a question about whether senders and recipients enjoy a reasonable expectation of privacy in the messages, and hence whether acquisition of them from an ISP or a telephone company is "electronic surveillance" or a "physical search" under FISA. Each of these three features – geography, storage, and the role of third parties – is considered in the discussion below.

ii. Acquisition of E-Mail (and Voice Mail) Under Current FISA.

The following paragraphs first address whether the acquisition of *stored* e-mail and voice mail is "electronic surveillance" (or a "physical search") as defined by FISA. They then address *transiting* e-mail.

Stored E-Mail. Stored e-mail and voice mail communications are neither "wire communications" nor "radio communications" under current FISA. As discussed above, the statute defines "wire communication" as a communication "while it is being carried by a wire."[162] Similarly, although the statute does not define "radio communication," every indication is that it includes communications only while they are being carried by radio wave. A stored communication – e-mail or voice mail – is not being carried by wire or radio wave,[163] and is therefore neither a wire nor a radio communication under current FISA. Subsections (1) – (3) of FISA's current definition of "electronic surveillance" apply only to "wire communications" and/or "radio communications."[164] Thus, acquisition of stored e-mail or voice mail is FISA "electronic surveillance," if at all, only under current Subsection (4).

For present purposes, current Subsection (4) requires two main elements: first, that there be the "installation or use" of a "surveillance device" in the United States "for monitoring to acquire information," other than from a wire or radio communication; and second, that the monitoring occur "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[165]

With respect to the first element of current Subsection (4), depending on the facts, acquisition of stored communications from an ISP or telephone company could involve a "surveillance device"; and if a surveillance device were involved, it would obviously be "installed or used."[166] It also seems likely that the acquisition of stored communications would involve "monitoring to acquire information." Obviously, when the government obtains copies of stored e-mails or voice mails it has "acquired information." Depending on the particulars of the acquisition, it would probably also involve "monitoring." There is a good argument that stored data as well as transiting data may be monitored: a grocery store clerk can monitor food items in the warehouse as well as on the shelves or in the check-out line. Reading an e-mail message stored on an ISP's server would be monitoring in the same way that reading a paper letter stored in a desk would be monitoring. There is also a good argument that monitoring need not be continuous: a doctor periodically monitors a patient's cholesterol as much as a lifeguard constantly monitors the water for swimmers in distress. Reading e-mails from a target's e-mail account once a day (or once a week) would be monitoring as much as reading them in real time as they arrive (although it is possible to imagine a court ruling otherwise). If a court determined that the first element were satisfied – i.e., that obtaining stored e-mail or voice mail involved the installation or use of a surveillance device for monitoring to acquire information – then the question would turn on the second element of the definition – i.e., whether this occurred in circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

On the other hand, if a court were to conclude that the acquisition of stored communications does *not* involve a "surveillance device" and/or "monitoring," and therefore is *not* "electronic surveillance," the court would then have to determine whether the acquisition satisfies FISA's definition of a "physical search." The current definition of a physical search also has two essential elements: first, it requires "any physical intrusion within the United States into premises or property … that is intended to result in a seizure, reproduction, inspection or alteration of information, material, or property"; and second, like current Subsection (4) of the definition of "electronic surveillance," it requires that the intrusion occur "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[167] The first element of the definition of "physical search" is plainly satisfied: obtaining copies of e-mails from an ISP's server (in the U.S.) requires a "physical intrusion" – or its equivalent under *Kyllo* – into the ISP's premises, and it clearly results in a "reproduction" of "information." The same is true with respect to acquisition of voice mails from the U.S. premises of a telephone company.

Thus, the dispositive question is the same whether acquisition of stored e-mail and voicemail is analyzed as electronic surveillance (because it involves "monitoring" with a "surveillance device") or a physical search (because it does not involve monitoring with a surveillance device but does involve a physical "intrusion" and a "reproduction" of "information"). The question is whether the surveillance or search occurs "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes."[168] That question is addressed below.

In general, law enforcement officials must get a warrant to acquire stored e-mail and voice mail.[169] With a few exceptions, the Stored Communications Act provides that an ISP or

telephone company may not voluntarily disclose, and that law enforcement cannot compel disclosure of without a warrant, the contents of stored communications if those communications are less than six months old, at least until they are retrieved by the recipient. The Act provides that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service," and also that "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant."[170] An ISP or a telephone company is clearly a provider of "electronic communication service"[171] to the public, and stored e-mails and voice mails are clearly in "electronic storage" in an "electronic communications system," at least until they are retrieved by the subscriber.[172] Thus, in light of the Stored Communications Act, "a warrant would be required" to acquire stored e-mails or voice mails for law enforcement purposes, and the operative question under FISA is whether such acquisition occurs "under circumstances in which a party has a reasonable expectation of privacy."

There is an argument under existing case law that neither the sender nor the recipient of an e-mail (or voice mail) message enjoys a reasonable expectation of privacy in the message. In *Smith v. Maryland*,[173] the Supreme Court rejected the argument that the "installation and use" of a pen register violated a defendant's "'legitimate expectation of privacy' regarding the numbers he dialed on his phone." The Court relied in part on the fact that the defendant had voluntarily conveyed the numbers to the telephone company:

> Telephone users ... typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.[174]

The Court in *Smith* tied its narrow holding to the broader principle that there is no legitimate expectation of privacy in information voluntarily provided to third parties, as reflected in some of its prior decisions, including *United States v. Miller*,[175] which found no reasonable expectation of privacy in records about a defendant's financial transactions maintained by his bank.[176] The Court in *Smith* stated that it "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[177] It went on to explain:

> In *Miller*, for example, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to ... banks and exposed to their employees in the ordinary course of business." .... Because the depositor "assumed the risk" of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private. This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner

> voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.[178]

Based on *Smith* and *Miller*, Congress in 1986 enacted the Stored Communications Act. As noted above, the Act provides statutory protection to stored communications, supplementing Title III's statutory protection for transiting communications, but it appears to be premised on the notion that such communications are not protected by the Fourth Amendment.[179] Indeed, certain provisions in the Act may be constitutional only if that is the case.[180]

If it were confronted with the constitutional question today, the Supreme Court might follow *Smith* and *Miller*, and reject any reasonable expectation of privacy for senders and recipients of e-mail and voice mail. However, the Court could find ways to distinguish both decisions if it wanted to.[181] Indeed, if it wanted to find a reasonable expectation of privacy in e-mail, the Court could rely on society's expectations derived from the Stored Communications Act itself,[182] or from the contractual arrangements between customers and their ISPs. One appellate court relied on an ISP's contractual arrangements and policies to find a reasonable expectation of privacy in e-mail.[183] Alternatively, Members of the Supreme Court more persuaded by common-law antecedents to the Fourth Amendment[184] could treat e-mail as the modern equivalent of postal mail, which has always been protected.[185] The issue is far from settled.[186]

Assuming for the moment that neither the sender nor the recipient of an e-mail or voice mail has a reasonable expectation of privacy in messages consigned to third parties, the third party itself – the ISP or telephone company – may have such an expectation that is relevant to FISA. Of course, the third party does not enjoy a reasonable expectation of privacy in the communication – e.g., in the e-mail's content. As noted above, however, the question under FISA is not confined to expectations of privacy in the content of acquired communications; it is whether the electronic surveillance or physical search conducted to acquire that content occurs under circumstances in which "a person" has a reasonable expectation of privacy. In most cases, the third party will retain a reasonable expectation of privacy in the place where the communications are stored and acquired.

Under Subsection (4) of the definition of "electronic surveillance," the precise question is whether "the installation or use" of the surveillance device occurs "under circumstances in which a person has a reasonable expectation of privacy."[187] Whether or not the "use" of the device to monitor a subscriber's e-mail would implicate an ISP's Fourth Amendment rights, certainly the "installation" of a device on its premises would do so. Thus, assuming that a "surveillance device" is installed and used for monitoring, acquisition of e-mails from an ISP is "electronic surveillance" under Subsection (4), either because the parties retain their expectation of privacy (despite *Smith* and *Miller*) in the content of the e-mail, or because the ISP retains its reasonable expectation of privacy in its e-mail servers where the surveillance device is installed.

A similar analysis applies under the definition of "physical search" if no surveillance device (or monitoring) is used. Apart from the "seizure, reproduction, inspection, or alteration"

that occurs once the government has arrived at the ISP or the telephone company, the "intrusion ... into premises or property" necessary to make the seizure would clearly implicate the third party's Fourth Amendment rights. Thus, acquisition of stored e-mail and voice mail (at least if unread and less than six months old) is either electronic surveillance or a physical search under FISA (it cannot be both).

Of course, if (based on *Smith* and *Miller*) the sender and recipient have no expectation of privacy in a stored communication, the third party could, as far as the Constitution is concerned, consent to its acquisition by the government and simply turn it over to the FBI upon request without the need for a warrant. However, as noted above, the Stored Communications Act generally forbids an ISP or telephone company from providing such consent.[188] Put another way, even with the third party's consent, a warrant would still be required for law enforcement purposes because of the Stored Communications Act. Thus, absent the consent of the sender or recipient, acquisition of stored e-mail or voice mail is "electronic surveillance" (or a "physical search") under FISA.[189]

Transiting E-Mail. As discussed above, e-mail differs from a telephone call in that it resides in electronic storage after being sent. The discussion thus far has analyzed acquisition of e-mail in storage. Acquisition of e-mail in real time, *before* the packets converge in the recipient's inbox, might or might not be "electronic surveillance," depending in the first instance on whether an ISP is a "common carrier" under FISA. There is no clear answer to this question in publicly-available materials, so it is necessary to address both possibilities.

If an ISP is not a common carrier, then e-mail transiting its wires or cables would not be a "wire communication" under FISA, and only current Subsection (4) would apply. Again, therefore, the question would reduce to whether a warrant is required to acquire transiting e-mail for law enforcement purposes. Although the Stored Communication Act would not govern – because transiting e-mail is not in storage – Title III itself requires a warrant to obtain transiting e-mail absent the consent of a party to the e-mail,[190] whether or not the party has a reasonable expectation of privacy under *Smith* and *Miller*.[191] Thus, absent the sender's or recipient's consent, using a surveillance device in the United States for monitoring to acquire transiting e-mail from an ISP that is not a "common carrier" under FISA would be "electronic surveillance."

Alternatively, if an ISP is a common carrier under FISA, then e-mail transiting its wires or cables would be a "wire communication," and current Subsection (2) – but not Subsection (4) – would apply.[192] Under Subsection (2), acquisition of the transiting e-mails would be "electronic surveillance" if either the sender or recipient were located in the United States, and neither party consented (or was a computer trespasser under Title III). The existence of a reasonable expectation of privacy would not matter. Absent the sender's or a recipient's consent, using a surveillance device in the United States to acquire transiting e-mail from an ISP that is a "common carrier" under FISA would be "electronic surveillance" if the sender or a recipient were in the United States.[193]

Finally, it is worth considering the results if, under any line of reasoning, acquisition of e-mail were held not to be "electronic surveillance" or a "physical search" under FISA. It would not leave the government free to acquire e-mail at will. On the contrary, it would mean that, as a

matter of statutory law,[194] the government generally could not acquire e-mail except by satisfying Title III, at least for domestic e-mails. That is because, as mentioned above, Title III generally prohibits interception of wire and electronic communications inside the United States absent consent and contains an exemption for conduct authorized by FISA.[195] Title III also contains an exemption for "acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978,"[196] but this exemption would not cover acquisition of domestic e-mail messages, and was enacted only to protect "certain international signals intelligence activities currently [as of 1978] engaged in by the National Security Agency."[197]

7. <u>The Government's Proposal</u>.

a. <u>Overview</u>.

It may be appropriate, before analyzing the government's proposal in detail, to focus on the motivations behind it. As far as I can tell, the government's proposal is animated by a desire not only to simplify the enormously complex definition of "electronic surveillance" in current FISA, but also to redress certain technological changes, and their legal consequences, that have occurred since the statute was enacted in 1978. In particular, the government has asserted publicly that FISA was not meant to reach most international (or at least transoceanic) communications because, in 1978, they were (generally) carried by radio rather than by wire.[198] As discussed above, under current FISA it is *not* "electronic surveillance" for the government to target a non-U.S. person by acquiring the contents of his international telephone calls while they are being transmitted as radio waves (rather than on a wire).[199] The government's argument, as I understand it, is that this exception was far more significant in 1978 than it is today, because – with the advent of fiber optic cables – international calls are now generally carried almost exclusively by wire, instead of by radio transmissions to and from satellites, leaving no opportunity for acquisition outside FISA's regulatory ambit.

I cannot comment further on this issue in this setting, but I do believe very strongly that it should inform any classified dialogue that ensues between Congress and the executive branch. Today's lawmakers obviously are not *bound* by the policy judgments of their predecessors in 1978, but I think they should make every effort to *understand* those judgments, and to determine how they have been affected by subsequent developments (technological or otherwise). These issues may be particularly important with respect to electronic mail, as discussed briefly below.

b. <u>The Proposed Definition of "Electronic Surveillance"</u>.

Section 401(b) of the government's proposal would simplify, and narrow, FISA's definition of "electronic surveillance." In place of four subsections, the new definition would have two: essentially, it would cover (1) surveillance targeting individuals (U.S.

persons and non-U.S. persons alike) in the United States who enjoy Fourth Amendment rights, and (2) surveillance of purely domestic communications (i.e., communications solely within the United States). In place of six relevant factors, the new definition would have four:

(1) the type of information being acquired ("information" in general or a "communication" of any type);

(2) the type of acquisition (e.g., through the use of a surveillance device or the installation of such a device, or otherwise);

(3) the location of the targets and others (reasonably believed to be inside or outside the United States); and

(4) the existence (or not) of a reasonable expectation of privacy and the need (or not) for a warrant to engage in the surveillance under law-enforcement rules.

Presented in a chart, the new definition would look like this:

Statute	50 U.S.C. § 1801(f)(1)	50 U.S.C. § 1801(f)(2)
Type of information	Any information	Any communication
Type of Acquisition	Installation or use of an electronic, mechanical, or other surveillance device	Intentional acquisition of contents of any communication
Targets	Surveillance intentionally directed at a particular, known person	Communication is from a sender to one or more recipients
Location of Targets	That person is reasonably believed to be located within the United States	Sender and all intended recipients are reasonably believed to be in the U.S.
Reasonable Expectation of Privacy (REP) and Warrant Required for Law Enforcement (LE) Purposes	That person has a REP and warrant required for LE purposes	A person has a REP and warrant required for LE purposes

As I understand the government's proposal, most of the terms in its definition of "electronic surveillance" would be read according to (or in contrast with) their closest analogues in current FISA. I review both proposed subsections of the government's definition below.

i. Proposed Subsection (1).

The first clause of proposed Subsection (1) refers to the "installation or use of an electronic, mechanical, or other surveillance device for acquiring information." This is very close to language in current Subsection (4), which refers to "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information." The difference, of course, is that the government's proposal eliminates two restrictions – "monitoring" and "in the United States" – which should expand, rather than contract, the scope of the provision. In any event, the first clause of proposed Subsection (1) should be read by analogy to the corresponding language in current Subsection (4), which is discussed at length in the analysis of current FISA above.

The second clause in proposed Subsection (1) – "by intentionally directing surveillance at a particular, known person who is reasonably believed to be located within the United States" – has an analogue in current Subsection (1), which now applies to surveillance of a wire or radio "communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person." Although the government has used slightly different words here, the concept of "intentionally directing surveillance" at a person is very close to the concept of "intentionally targeting" that person.[200] The "reasonably believed" modifier is probably intended to protect the government from liability in the event that it makes a (reasonable) error in determining the location of the target. As discussed above, electronic mail and mobile telephones raise geographical issues not present where landline telephones are concerned.

As discussed above, the reference to a "particular, known" person in current Subsection (1) is meant to cover watchlisting and similar activities, and – in my view – applies to any deliberate use of a surveillance device to monitor a specific communications channel where the but-for purpose of the surveillance is to acquire communications from a U.S. person in the U.S. As further discussed above, however, the remaining subsections of the current definition generally absorb any slack that arises from uncertainty about the meaning of this language.[201] For that reason, it would be of the utmost importance, before enacting the government's proposal, to ensure a common understanding of what it means to "intentionally direct[] surveillance at a *particular, known* person." The precise question is whether the government believes that proposed Subsection (1) excludes wide-ranging or "driftnet" surveillance, on the theory that the target of such surveillance is *all* persons (or a group of persons, or persons in general), rather than any "particular, known" person. If the government takes that position, its proposal (if enacted) would mean that a surveillance program like Operation Shamrock would be unregulated by FISA.[202]

In all candor, I cannot believe the government will take that position. I suspect, rather, that proposed Subsection (1) is meant to cover any surveillance that is intentionally directed at *any* person or persons – particularly known or otherwise – who are reasonably believed to be located within the United States. If that is the case, it may be possible to dispel any uncertainty by changing the language of proposed Subsection (1) in exactly that

way. In any event, to repeat, the issue should be resolved authoritatively so that no question remains for the future.

The third and final phrase in proposed Subsection (1) – "under circumstances in which that person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" – differs from its closest analogue in current FISA because of its reference to "that person" rather than "a person." As discussed above, current Subsections (1), (3), and (4) apply when "a person" has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;[203] as a result, the reasonable expectation of privacy does not depend on the status of the particular individual whose privacy is being invaded by the surveillance.[204]

By referring to "that person," however, proposed Subsection (1) apparently would apply only when there is a reasonable expectation of privacy in the "particular, known" person at whom the surveillance is directed. Depending on the Fourth Amendment rights of non-U.S. persons in the United States, as discussed with respect to current FISA above, the government's proposal might not regulate surveillance of international communications targeting (certain) non-U.S. persons in the United States. Similarly, it might not regulate microphone or video surveillance of such persons, as long as the surveillance is not intentionally directed at their "communications" rather than other activities. That is because proposed Subsection (1) would not apply to the extent that non-U.S. persons do not enjoy Fourth Amendment rights, and proposed Subsection (2) – which follows the traditional approach in referring to "a person" – applies only to intentional surveillance of purely domestic communications, not to international communications, and not to any non-communicative conduct.[205]

This too strikes me as an issue that should be resolved firmly before enacting (or in the text of) any legislation. I note that here, too, any uncertainty would be eliminated if proposed Subsection (1) were changed to refer to *any* person or persons who are reasonably believed to be located in the United States, under circumstances in which *a* person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

ii. Proposed Subsection (2).

The first clause of proposed Subsection (2) refers to "the intentional acquisition of the contents of any communication." This is drawn from current Subsection (3), which applies to "the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication." The reference to "intentional" acquisition, I think, is meant to exclude accidental, but inevitable, overcollection. If anything, I believe, such accidental overcollection is more of a problem today than it was in 1978, because of the proliferation of communications and communications technologies. One important change, of course, is that Section 401(e) of the government's proposal narrows the definition of "contents" to exclude routing and addressing information. As amended, contents would include only the "substance, purport, or meaning" of the communication, as is currently the case under Title III.

This is an interesting issue, but not one that I have had time to address at any length in these comments.

The second clause of proposed Subsection (2) – "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes" – is identical to the language in current FISA, and would be given the same meaning.

The third and final clause of proposed Subsection (2) restricts the provision to situations in which "the sender and all intended recipients are reasonably believe to be located within the United States." This obviously excludes any international communications – or any communications reasonably believed to be international.

c. Application of the Proposed Definition.

The government's proposed definition of "electronic surveillance," although simpler than current law, is still complex. Set out below are several hypothetical examples that may help illustrate the meaning of the definition as applied to particular facts or scenarios.

i. Traditional Land-Line Telephone Calls.

It is "electronic surveillance" under proposed Subsection (2) if the government intentionally acquires the contents of any telephone communication – mobile, cordless, or landline – between a person of any nationality reasonably believed to be in one state, Mr. *A*, and another person of any nationality reasonably believed to be in the same or another state, Ms. *B* (it does not matter who called whom). That is because proposed Subsection (2) applies to the intentional acquisition of the contents of "any" domestic communication in which there is a reasonable expectation of privacy and a warrant would be required for surveillance for law enforcement purposes. Subsection (1) also would apply to such surveillance, if the surveillance is effected using a device, and if the target of the surveillance – *A* or *B* – has a reasonable expectation of privacy (e.g., because of status as a U.S. person).

If *B* is located abroad instead of in the United States, then proposed Subsection (2) does not apply. However, if *A* is the target, and has a reasonable expectation of privacy, and if the surveillance is effected by a device, then the surveillance would be "electronic surveillance" under proposed Subsection (1). If both *A* and *B* are abroad, surveillance of their call would not be "electronic surveillance," as is the case under current law.

As noted above, there may be some uncertainty about "driftnet" surveillance of international calls, which would not be covered under proposed Subsection (2), to the extent that such surveillance is not considered to be intentionally directed at a "particular, known" U.S. person, within the meaning of proposed Subsection (1).

ii. Faxes.

Fax communications that transit conventional telephone lines should generally be indistinguishable from spoken telephone conversations under the government's proposal.

Although a fax message is not an aural communication, like a telephone call, it is a "communication" under the government's proposal.

iii. Mobile Telephone Calls.

Mobile telephones obviously raise geographical issues. When the government conducts surveillance of traditional land-line telephones (or fax machines), it knows where the telephone is located – that is the distinguishing feature of a land line. Thus, when the government monitors *A* talking (or faxing) on his home telephone, it can be reasonably confident that he is in fact at his home address. In such a case, the government can therefore know, in advance, that the surveillance targeting him will be subject to proposed Subsection (1) if that home address is in the United States (at least to the extent that *A* has Fourth Amendment rights).

When *A* is using a mobile telephone, however, he may be virtually anywhere, including outside the United States. When the government applies for a FISA order on *A*'s mobile telephone, it cannot know, in advance, whether or not he will use it to make calls from within the United States. Caution dictates obtaining a FISA order, of course, unless the government can be sure that *A* is in fact out of the country, but to the extent that *A* takes a temporary trip abroad, surveillance of calls made from his mobile phone would not be "electronic surveillance" under the government's proposal.

iv. Microphones and Video.

If the government has a microphone concealed where *A* or *B* is located when making a private call (using any kind of telephone or other device), and the microphone acquires at least one side of the conversation, it is electronic surveillance under proposed Subsection (1) if the target – *A* or *B* – is located in the United States and enjoys a reasonable expectation of privacy. That is the case whether or not *A* and *B* are U.S. persons, and regardless of where the microphone is located. The same holds true for microphone or video surveillance of *A* or *B* if they are engaged in an oral communication or even if they are not engaged in a conversation; "electronic surveillance" under proposed Subsection (1) applies to the acquisition of "information," not merely "communications."

v. E-Mail and Voice Mail Messages.

Electronic mail and voice mail messages raise difficult practical and legal issues under the government's proposal, but the issues may be different, and perhaps less amenable to public discussion, than those raised under current FISA. The discussion below assumes familiarity with the explanation of e-mail in the analysis of current FISA above.

Although stored e-mail is not a "wire communication" or a "radio communication" under current FISA, it probably is a "communication," and transiting e-mail certainly is a "communication." Thus, surveillance of the contents of such e-mail satisfies the first clause of proposed Subsection (2). The next clause of the proposal concerns whether "a person" has a reasonable expectation of privacy in the e-mail message, and whether a warrant

would be required to acquire the contents of the e-mail for law enforcement purposes.[206] For now, it is appropriate to assume, based on the earlier discussion of the same issue under current FISA, that this clause is satisfied. That leaves the third and final clause of Subsection (2), which turns on whether the "sender and all intended recipients" of the e-mail are reasonably believed to be located in the United States. This raises technically complex – and somewhat metaphysical – questions that I am not at liberty to discuss here.[207] I recommend that Congress take up the issue with the executive branch in detail in an appropriate closed session. The same applies with respect to analysis under proposed Subsection (1), at least if the target of the surveillance is located in the United States.

8. Intersection With Title III.

By narrowing the definition of "electronic surveillance" in FISA, the government's proposal may raise issues under Title III, the criminal wiretapping statute. Title III sets out a broad rule against electronic surveillance and the use or disclosure of information obtained from electronic surveillance "[e]xcept as otherwise specifically provided in this chapter."[208] In particular, Title III generally prescribes criminal penalties for anyone who (1) "intentionally *intercepts*, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication";[209] (2) "intentionally *discloses*, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection";[210] or (3) "intentionally *uses*, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection."[211]

Title III's definitions[212] mean that its general prohibition on the interception of wire, oral, and electronic communications includes almost all of what FISA currently defines as "electronic surveillance"[213] conducted inside the United States. Correspondingly, Title III's general prohibition on use or disclosure of information obtained from such interceptions therefore includes uses or disclosures authorized under FISA and FISA minimization procedures. Thus, the issue arises whether Title III forbids what FISA expressly permits.

Fortunately, under current law, a conflict between the statutes is averted because Title III explicitly authorizes electronic surveillance under FISA:

> Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.[214]

Thus, Title III's general prohibition of the interception of wire, oral, or electronic communications, and its derivative prohibitions of the use or disclosure of information obtained from unauthorized interceptions, do not apply to "electronic surveillance" authorized by the

current version of FISA, or to the use or disclosure of information obtained from such "electronic surveillance."

If Section 401(b) of the government's proposal were enacted, Title III's exception authorizing "electronic surveillance" as defined by FISA would be narrowed – because FISA's definition of "electronic surveillance" would be narrowed – and to that extent there might be a conflict between the two statutes. Some (if not most) of that conflict will be resolved by 18 U.S.C. § 2511(2)(f),[215] and by Section 402 of the government's proposal (discussed below, which authorizes conduct that is *not* "electronic surveillance" under FISA, and which applies "notwithstanding any other law"), but I would need a few more hours to work through all of the legal and operational possibilities to be sure. I assume the government already has done that, but it is an issue that should be very carefully considered.

Section 402

Section 402 of the government's proposal would significantly expand the Attorney General's power to authorize electronic surveillance of foreign powers without judicial review under 50 U.S.C. § 1802. This would be another very significant change in the law.

1. Background on Current 50 U.S.C. § 1802.

Under the current version of 50 U.S.C. § 1802, the government may conduct electronic surveillance of certain foreign powers without judicial approval. The statute provides that "[n]otwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order ... to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath" three essential requirements.[216]

The first requirement is exclusivity: the electronic surveillance must be directed solely at communications channels used exclusively by official foreign powers, or at acquisition of technical intelligence from property "openly and exclusively controlled" by official foreign powers, and the physical search must also be directed solely at such property or at property "used exclusively" by official foreign powers. The second requirement is that there be "no substantial likelihood" that the search or surveillance will infringe on a U.S. person's privacy interests. Third and finally, the surveillance or search must be conducted in accord with minimization procedures that are reported to Congress. The Attorney General's certification of these three elements must be transmitted to the FISC for safekeeping, although the FISC does not review the certification.[217] The Attorney General may also direct a specified communications common carrier, landlord, or other specified person to assist in implementing the surveillance or search and to maintain records pertaining to the surveillance or search under proper security procedures.[218]

Before discussing each of the three requirements in detail, it is worth noting that Sections 1802 and 1822 reflect a political compromise, crafted in 1978, between those who believed that "a warrant should be required across-the-board" for all electronic surveillance under FISA, and those who "felt that a judge should never be involved."[219] In

the end, the "consensus" was that "a judicial warrant should be required whenever the Fourth Amendment rights of Americans might be involved."[220] Based on testimony "taken in closed session, [the House Intelligence] committee determined that there was a class of surveillances, otherwise within the scope of the bill, where there was little or no likelihood that Americans' Fourth Amendment rights would be involved in any way. The committee also determined that this class of surveillances included some of the most sensitive surveillances which this Government conducts in the United States."[221] The result was Section 1802, and later its counterpart for physical searches, Section 1822.

a. Exclusive Use or Control by an Official Foreign Power.

Under current Section 1802, the electronic surveillance must be "solely directed at" acquisition of "the contents of communications transmitted by means of communications used exclusively between or among foreign powers,"[222] or acquisition of "technical intelligence other than the spoken communications of individuals, from property under the open and exclusive control of a foreign power."[223] (Under Section 1822, the physical search must be "solely directed at" the "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers."[224])

The "foreign powers" in question under both provisions must be "official" foreign powers as defined in 50 U.S.C. §§ 1801(a)(1)-(3).[225] That is, they must be "a foreign government or any component" of a foreign government; a "faction" of a foreign nation or nations "not substantially composed of U.S. persons," such as the PLO;[226] or an entity "openly acknowledged" by a foreign government or governments to be "directed and controlled" by those government or governments, such as a state airline or OPEC.[227] Sections 1802 and 1822 do not extend to other foreign powers, such as international terrorist groups.

Sections 1802 and 1822 apply to property or premises under the "open and exclusive control" of foreign powers (and Section 1822 also applies to physical searches of property "used exclusively by" foreign powers).[228] This would cover a foreign government's embassy or diplomatic mission, or other facilities owned by an official foreign power from which outsiders may be excluded.[229] Both provisions currently authorize the surveillance or search "notwithstanding any other law," and the statute's 1978 legislative history explains that the phrase was used in FISA to make clear that "the activities authorized in the bill are not prohibited by the Vienna Convention on Diplomatic Relations."[230] The Vienna Convention establishes protocols under which "sending States" establish diplomatic missions in "receiving States," provides that the "premises of the mission shall be inviolable," and in particular provides that the "agents of the receiving State may not enter them, except with the consent of the head of the mission."[231] Sections 1802 and 1822 seem clearly to contemplate violations of the Vienna Convention.[232] In 2003, the Department of Justice wrote in a draft summary of proposed legislation that "[i]n essence, § 1802 authorizes the surveillance of communications between foreign governments, and between a foreign government and its embassy."[233]

Section 1802 also applies to acquisition of "technical intelligence, other than spoken communications of individuals," acquired from such exclusively controlled property. The term

"technical intelligence" is not defined in the statute, and the legislative history warns that it "cannot elaborate on the activities covered" by this provision.[234] Nor can I.

b. No Substantial Likelihood of Surveilling or Searching U.S. Persons.

In addition to the first requirement, concerning exclusivity, both Section 1802 and Section 1822 today contain a second requirement, in that they apply only where there is "no substantial likelihood" that the electronic surveillance will acquire the contents of any "communication to which a U.S. person is a party" or that the search will involve the "premises, information, material, or property" of a U.S. person.[235] This second requirement directs the government to predict the likelihood of infringing on U.S. person privacy interests, with the Attorney General certifying the prediction "in writing under oath."[236]

To some degree, the second requirement duplicates the first. If a communications system is indeed used exclusively by official foreign powers, then the odds of acquiring communications to or from a U.S. person seem remote. But there may be cases in which the second requirement operates independently. For example, a "foreign power" as used in Sections 1802 and 1822 includes a "faction" of a foreign nation such as the PLO.[237] Such a faction may include some U.S. persons, as long as they do not make up a "substantial" portion of the faction.[238] If such a faction, partially but not substantially composed of U.S. persons, had open and exclusive control of premises in the United States, the first requirement of Sections 1802 and 1822 would be satisfied, but the second requirement might not be.

c. Minimization.

A surveillance or search under current Sections 1802 and 1822 must be conducted in accordance with "minimization procedures" that meet the statutory requirements and that are reported in advance, or promptly after the fact where necessary, to the House and Senate Intelligence Committees.[239] The Attorney General must also assess compliance with the minimization procedures and report on the assessment as part of the semi-annual report to the Intelligence Committees.[240]

Minimization procedures must address the possibility that, despite the Attorney General's expectations and certification under oath, a surveillance or search may acquire or involve a U.S. person's communications or property. If that occurs, the government must obtain an approval order from the FISC. The statute currently provides that such information may not be retained or used "for any purpose" for longer than 72 hours unless "a court order" approving the surveillance or search "is obtained" or unless the Attorney General determines that "the information indicates a threat of death or serious bodily harm to any person."[241] As a technical matter, this means that the government must file its application, and the FISC must issue its order, within 72 hours after the U.S. person information is acquired. Even if the government timely files the application, if the FISC does not rule and issue its order quickly, the information would need to be destroyed (absent a threat of death or serious bodily harm).

2. The Government's Proposal.

Under the government's proposal, Section 1802 would be expanded significantly. It would apply to surveillance "directed at," rather than "solely directed at," an official foreign power, and to surveillance of all communications of such a foreign power rather than communications made on facilities used "exclusively between or among foreign powers." In other words, the provision apparently would apply to *any* communications facility used by, or about to be used by, a foreign power.[242] Correspondingly, the government's proposal would eliminate the requirement that there be "no substantial likelihood" of acquiring a U.S. person's communications. If surveillance is to include facilities used by U.S. persons, then the Attorney General obviously cannot certify that U.S. persons will not be surveilled. And, of course, Section 401(d) of the government's proposal deletes current 50 U.S.C. § 1801(h)(4), the minimization provision that effectively requires sequestration of U.S. persons' communications which are (despite expectations) acquired under current 50 U.S.C. § 1802.

Section 402 of the government's proposal would also enact new 50 U.S.C. § 1802A, which applies to the acquisition of foreign intelligence information using methods that are *not* "electronic surveillance" under certain circumstances. The circumstances would be (1) that the surveillance is to acquire foreign intelligence information "concerning persons reasonably believed to be outside the United States"; (2) that the information be obtained from a communications provider or other third party; (3) that a significant purpose of the surveillance be to obtain foreign intelligence information; and (4) that proper minimization procedures be followed. Where these conditions are met, Section 402 of the government's proposal would allow the Attorney General to authorize surveillance (and other collection) activity without a court order for one-year periods.

This provision, which applies only to conduct that is *not* "electronic surveillance" as defined by FISA, obviously takes on added significance when paired with the narrowing of that definition in Section 401(b) of the government's proposal. As discussed above, Section 401(b) might exclude from "electronic surveillance" certain kinds of non-targeted "driftnet" surveillance of international communications. To the extent that is the case, those kinds of surveillance would be within the scope of 50 U.S.C. § 1802A as proposed by the government. Indeed, proposed 50 U.S.C. § 1802A(b), which provides that the surveillance need not be confined to a particular communications facility, seems to confirm the breadth of the provision. The provision seems designed for collection wholesale – it seems to signal this intention by providing explicitly that it applies *only* to acquisition from or with the assistance of communications providers. It would be very important to determine how proposed Section 1802A would affect existing or contemplated surveillance activity like the (judicial or non-judicial versions of the) Terrorist Surveillance Program (TSP).

Proposed Section 1802A applies only to the acquisition of foreign intelligence information "concerning" persons reasonably believed to be abroad, and only when there is a "significant purpose" to obtain foreign intelligence information. This does not mean that it requires the surveillance *targets* to be abroad, but only that the information obtained

concern someone (reasonably believed to be) abroad. Moreover, it may be that acquisition of such information need only be a significant purpose of the surveillance, arguably leaving room for the primary purpose to be acquisition of other types of foreign intelligence information.[243]

Finally, it is also worth noting that this provision could be read as a Congressional endorsement of one-year periods of surveillance for U.S. persons under Section 2.5 of Executive Order 12333.[244] The statute would not resolve the "reasonableness" of such surveillance, of course, but it would probably have some influence on a judicial determination of that Fourth Amendment question.

I have not examined closely the elements of proposed 50 U.S.C. § 1802B, which would allow the Attorney General to compel assistance from a third party provider. This handmaiden provision probably should rise or fall with proposed 50 U.S.C. § 1802 and 1802A, and any technical errors should be relatively easy to repair. (It may be the case that, even if 50 U.S.C. § 1802 remains unchanged, the government needs some sort of compulsory provision directed at communications providers; if that is the case then proposed Section 1802B might still be useful.)

Nor have I examined closely proposed 50 U.S.C. § 1802C, which appears to import FISA's suppression and discovery provisions to surveillance conducted under proposed 50 U.S.C. § 1802A. Again, this provision rises or falls with 50 U.S.C. § 1802A, and should be relatively straightforward as a technical matter.

Section 403

This provision makes sense to me. Adding "at least" before the reference to seven circuits is appropriate now that the FISC consists of eleven (rather than seven) judges. The Chief Justice, who appoints judges to the FISC, has (correctly) interpreted the statute that way since the USA PATRIOT Act, but it is wise to make the matter explicit. Nor do I see any problem with moving what is now 50 U.S.C. § 1802(b) into 50 U.S.C. § 1803. I would consider changing "the purpose" to "a significant purpose" in the moving language, but I do not consider it essential. I note the absence of the requirement that the President have, by written designation, empowered the Attorney General to approve applications to the FISC, but if such a provision raises separation-of-powers concerns, I have no strong objection to its omission.

Section 404

Section 404 of the government's proposal would reduce the required elements of an ordinary FISA application for electronic surveillance. It may therefore be helpful to begin with a description of the current requirements of such an application.

1. Current Law Governing FISA Applications.

Under current law, applications for court orders authorizing electronic surveillance or physical searches (or both[245]) under FISA are made to the FISC under oath by a federal officer with the approval of the Attorney General, the Acting Attorney General, the Deputy Attorney

General, or – if designated by the Attorney General – the Assistant Attorney General for National Security.[246] Typically, such an application includes statements made by an attorney in the Office of Intelligence Policy and Review (OIPR), a component of the Department of Justice[247] that represents the federal government before the FISC, as well as an affidavit (referred to in the government as a "declaration") from an investigating agency such as the FBI.[248]

a. Contents of Application.

To meet the statutory requirements in current FISA, the application must provide the identity of the applicant[249] and include information concerning the following (items marked with an asterisk, rather than a bullet point, would change if Section 404 of the government's proposal were enacted):

- *Who is being searched or surveilled.* The application must include the "identity, if known, or a description of the [specific] target."[250]

- *Why the target lawfully may be searched or surveilled.* The application must include a statement of facts that is "relied upon by the applicant to justify his belief,"[251] and used by the FISC to determine probable cause, that the target of the surveillance or search is a "foreign power" or an "agent of a foreign power."[252]

- *A nexus between the target and the location of the search or surveillance.* In electronic surveillance cases, the application must include a statement to establish that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[253] In physical search cases, it must include a statement to establish that "the premises or property to be searched contains foreign intelligence information,"[254] and that it "is owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power."[255]

- *A description of what is to be searched or surveilled.* In electronic surveillance cases, the application must include a description of "the type of communications or activities to be subjected to the [electronic] surveillance."[256] In physical search cases, it must include a "detailed description of the premises or property to be searched and of the information to be seized, reproduced, or altered."[257]

* *The nature of the information sought by the search or surveillance.*[258]

- *Limits on the search or surveillance.* The application must contain a statement of "proposed minimization procedures."[259]

* *An explanation of how the search or surveillance will be carried out.* In electronic surveillance cases, the application must include a statement of "the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance."[260] In physical search cases, it must include a description of "the manner in which the physical search is to be conducted."[261] In addition, in physical

search cases only, the government must file a return with the FISC upon completion of the search that reports its "circumstances and results."[262]

* *An account of any prior FISA applications.* The application must include a statement "concerning all previous applications" involving any of the persons, facilities, places, premises, or property specified in the current application, and the action taken on each previous application.[263]

In addition, in electronic surveillance cases only, the application must also include statements concerning the following two additional matters:

* "[T]he period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter."[264]

* "[W]henever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device."[265]

b. Mechanics and Accuracy of Application.

As the FBI observed in the spring of 2001, "[i]n recent years, applications for electronic surveillance or physical search authority submitted to the [FISC] have evolved into increasingly complex documents. The heart of these applications is the declaration, signed by a supervisory special agent at FBIHQ [FBI Headquarters in Washington, D.C.], which sets out the factual basis supporting probable cause for the requested authority and which conveys to the FISC any other facts relevant to the Court's findings."[266] This observation highlights an important distinction between FISA applications and applications for search warrants and Title III orders used in conventional criminal investigations. Unlike an ordinary search warrant or Title III order, which can be issued by a local federal judge in any judicial district, FISA orders are issued only by the FISC, a court that sits in Washington, D.C. In part because the FISC's practice is often to have the declarant appear in person, and in part because of the coordinating role played by FBIHQ in NSIs, the FISA declaration is typically signed by a headquarters agent.[267]

This creates a potential problem: although the FISA declarant resides in Washington, D.C., the facts in the declaration may nonetheless pertain to NSIs being conducted in any FBI field office, from Seattle to Miami. As the FBI has explained, "[t]he information currently required for a FISA declaration, in many cases, is extensive, and often includes descriptions of operations, criminal investigations, or prosecutions well outside the personal, or even programmatic, knowledge of the Headquarters supervisor who will serve as the declarant."[268] Procedures adopted by the FBI in April 2001 (and later declassified) are designed to "ensure accuracy" in FISA declarations concerning the facts supporting probable cause, the nature of

related criminal matters; and the "existence and nature of any prior or ongoing asset relationship between the subject [i.e., the FISA target] and the FBI."[269]

These so-called "Woods Procedures," named after the capable FBI attorney who was their principal drafter, require FBI agents in the field and at headquarters to (1) search electronic databases and files for references to the FISA target, document the results of those searches, and complete a "FISA Verification Form"; (2) review, edit, and approve the declaration for factual accuracy; and (3) collect all relevant documentation of the required reviews. In cases where multiple field offices may be involved, each field office must review the application. In cases where criminal investigations are being conducted, the criminal agents must also review relevant portions of the declaration.[270] The procedures are elaborate and exacting, but they appear to have worked well.[271]

c. Certification.

To obtain approval for electronic surveillance or physical search under current law, the government must also submit to the FISC a written certification from a high-ranking executive branch official.[272] The only certifying official specifically mentioned in FISA is the "Assistant to the President for National Security Affairs" – commonly referred to as the National Security Advisor.[273] Other persons may certify only if they are "an executive branch official ... designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate."[274] Typically, the Director of the FBI certifies FISA applications from the FBI,[275] and the Secretary or Deputy Secretary of Defense certifies applications from the NSA.[276] (As discussed below, Section 404 of the government's proposal would change the permissible rank of the certifying official to include any federal official.)

Under current law, the certification must do all of the following (items marked with an asterisk, rather than a bullet point, would change if Section 404 of the government's proposal were enacted):

- **State that the certifying official "deems" the information sought to be "foreign intelligence information."[277]**
- **State that a "significant purpose" of the electronic surveillance or physical search is to obtain foreign intelligence information.[278]**
- **State that such information "cannot reasonably be obtained by normal investigative techniques."[279]**
- * **Designate "the type of foreign intelligence information being sought according to the categories described in" the definition of "foreign intelligence information."[280]**

Under current law, the certification must also include "a statement of the basis" for the latter two elements – that the information sought is the type of foreign intelligence

designated and that it cannot reasonably be obtained by normal investigative means.[281] (This too would change under the government's proposal.) The certification is effectively an affidavit,[282] and the 1978 House report on FISA explains that its purpose is to

> **insure that a high-level official with responsibility in the area of national security will review and explain the executive branch determination that the information sought is in fact foreign intelligence information. The requirement that this judgment be explained is to insure that those making certifications consider carefully the cases before them and avoid the temptation simply to sign off on certifications that consist largely of boilerplate language. The committee does not intend that the explanations be vague generalizations or standardized assertions.... The designated official must similarly explain in his affidavit why the information cannot be obtained through less intrusive techniques. This requirement is particularly important in those cases when U.S. citizens or resident aliens are the target of the surveillance.[283]**

Where the FISC is dissatisfied with the certification, it can require additional certifications.[284]

d. Attorney General Approval.

The final element in a FISA submission seeking an electronic surveillance or physical search order from the FISC is the citation of the Attorney General's authority, conferred by the President, to file FISA applications,[285] and the Attorney General's written approval of the particular FISA application being filed "based upon his finding that it satisfies" the statutory requirements.[286] The 1978 legislative history of FISA explains the purpose of this approval requirement:

> Each application must be approved by the Attorney General, who may grant such approval if he finds that the appropriate procedures have been followed. The Attorney General's written approval must indicate his belief that the facts and circumstances relied upon for the application would justify a judicial finding of probable cause that the target is a foreign power or an agent of a foreign power and that the facilities or place at which the electronic surveillance is directed are being used, or about to be used, by a foreign power or an agent of a foreign power, and that all other statutory criteria have been met. In addition, the Attorney General must personally be satisfied that the certification has been made pursuant to statutory requirements.[287]

This is a heavy responsibility, but the Attorney General need not face it alone. If necessary, the Attorney General may "require any other affidavit or certification from any other officer in connection with the [FISA] application."[288]

On the other side of the balance, in certain cases, another high-ranking executive branch official may force the Attorney General's personal involvement in reviewing a FISA application.

Under two provisions of the current statute, "the Attorney General shall personally review" a FISA application for electronic surveillance or physical search of certain FISA targets upon written request from the Director of the FBI, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence (DNI).[289] This obligation is not delegable by the Attorney General (or any of the other officials mentioned) except "when disabled or otherwise unavailable."[290] If the Attorney General does not approve the application, he or she must give written notice to the requesting official and explain the changes needed to secure approval.[291] The requesting official must then modify the application if he or she believes it is appropriate to do so.[292] As discussed below, the government's proposal would add the Director of the CIA to the list of officials covered by this provision.

In physical search cases involving "the residence of a United States person,"[293] the Attorney General must also "state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information."[294]

As enacted in 1978, FISA defined "Attorney General" to include the Attorney General, the Acting Attorney General, or the Deputy Attorney General. In 2006, the statute was amended to provide that the "Attorney General" also includes the Assistant Attorney General for the National Security Division, if designated by the Attorney General.[295]

2. <u>The Government's Proposal.</u>

The most significant part of Section 404 of the government's proposal would change the permissible status of the certifying official. It would allow the President to designate *any* executive branch official as the certifier. Presumably, this is designed to let the President designate one or more NSA shift supervisors or other mid-level managers. While I can see the need to expand the roster of certifying officials, under current law the President is free to do so by naming any Senate-confirmed official. The burden of persuasion that the government needs a broader and lower-ranking pool of candidates should be relatively high, in my opinion, because the inevitable risk of such a move is to denigrate the significance of the certification.

Section 404 also would eliminate the requirement that "whenever more than one electronic, mechanical or other surveillance device is to be used with respect to a particular proposed electronic surveillance, the coverage of the devices involved and what minimization procedures apply to information acquired by each device."[296] I can understand the government's aversion to this provision, but I would not jettison it lightly, at least without some explanation.

Other changes in Section 404 of the government's proposal are less significant. Section 404 would eliminate the requirement, now totally boilerplate, that every FISA application recite the authority conferred on the Attorney General by the President to make the application.[297] This is similar to the change in Section 403 of the government's proposal discussed above; it provokes no strong reaction in me. The various changes from "detailed statement" to "summary statement" may not be very significant in operational effect, because the FISC will still be able to demand the level of detail that it finds appropriate.

Section 405

As time was running out on this project, I quickly scanned Section 405 of the government's proposal. As far as I can tell, apart from making changes corresponding to Section 404, it does the following. **First, it increases the duration of certain surveillance of non-U.S. persons who are agents of foreign powers, and (unless I am misreading) it may allow one-year renewal periods even for U.S. persons. It also increases the duration of emergency surveillance to one week, and – to my surprise – seems to suggest that the Attorney General must personally notify the FISC when he authorizes such surveillance (because it seems to delete any reference to his "designee" – perhaps general delegation principles are thought to make that superfluous). It appears to eliminate any second-guessing of the Attorney General's use of emergency surveillance, removing the word "reasonably" before "determines" in current 50 U.S.C. § 1805(f), and adding "determines that" before "the factual basis exists" in current 50 U.S.C. § 1805(f)(2).** And it expands the circumstances in which the "take" from unratified emergency surveillance may be used.

Section 406

Section 406 of the government's proposal may take on added significance with the amendments to the definition of "electronic surveillance" contained in Section 401(b) of the government's proposal. I have no objection to the government's preservation of its privileges in the paragraph (2) of the proposal.

Section 407

Section 407 of the government's proposal addresses weapons of mass destruction. It would expand the definition of "foreign power" to include a group engaged in the "international proliferation of weapons of mass destruction," expand the definition of "agent of a foreign power" to include a non-U.S. person who engages in such proliferation, and expand the definition of "foreign intelligence information" to include information necessary or relevant to the ability of the United States to protect against such proliferation. Conceptually, this provision may make sense – i.e., there may be examples, available for discussion in a classified setting, of cases where weapons of mass destruction, but *not* terrorism, are involved. **I am uncertain, however, about the breadth of the definition of "weapon of mass destruction"; for example, it seems to include even a very large caliber semiautomatic handgun.**[298]

Section 408

I have no comment on this provision.

Section 409

I assume (but have not checked) that this provision, which applies to physical searches, corresponds to the changes made in other provisions of the proposal that govern electronic surveillance. If so, most of my comments above would apply. It would be important to ensure

that the government has worked through the relationship between the definition of "electronic surveillance" and the definition of "physical search."

Section 410

If emergency electronic surveillance is to endure for a week, under Section 405 of the government's proposal, then it makes sense to apply the same standard to pen/trap surveillance.

Section 411

I have no comment on this provision.

Section 412

I did not read this provision, taking seriously the title's assertion that it contains only "technical and conforming amendments."

Section 413

I have no comment on this effective date provision of the statute.

Section 414

I have no comment on this severability provision of the statute.

* * *

Thank you very much for the opportunity to comment on this interesting proposal.

Sincerely,

David S. Kris

P.S. The notes begin on the next page.

NOTES

[1] I was first contacted about providing comments on the afternoon of Wednesday, April 25. As a former government employee, I submitted an initial draft of this letter to the Department of Justice (DOJ) on Friday morning, April 27, and subsequent drafts over the course of the weekend, for prepublication review under 28 C.F.R. § 17.18. I am grateful to DOJ for its extremely rapid review. This letter reflects only my own views, not those of any other person or entity, including DOJ. Some of the material in this letter is derived from a treatise that I co-authored with Doug Wilson, *National Security Investigations and Prosecutions*, which is forthcoming from Thomson-West publishing.

[2] H.R. Rep. No. 95-1283, Part I, at 68 (1978) [hereinafter FISA House Report].

[3] The electronic surveillance provisions of FISA, enacted in 1978, refer to "his belief." 50 U.S.C. § 1804(a)(4). The physical search provisions, enacted in 1994, are gender neutral and refer to "the applicant's belief." 50 U.S.C. § 1823(a)(4).

[4] 50 U.S.C. § 1804(a)(4)(A) (electronic surveillance); 50 U.S.C. § 1823(a)(4)(A) (physical search). Correspondingly, to approve the FISA application, the FISC must find probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3)(A) (electronic surveillance); 50 U.S.C. § 1824(a)(3)(A) (physical search).

[5] The certification provisions are at 50 U.S.C. § 1804(a)(7) (electronic surveillance) and 50 U.S.C. § 1823(a)(7) (physical search). The definition of "foreign intelligence information" is at 50 U.S.C. § 1801(e).

[6] 18 U.S.C. § 2510 et seq. For a more complete discussion of the FISA application process, see my comments on Section 404 of the government's proposal, below.

[7] See 50 U.S.C. § 1801(a) and (b).

[8] 50 U.S.C. § 1801(a)(4) ("a group engaged in international terrorism or activities in preparation therefor").

[9] See FISA House Report at 67 ("while it is expected that most entities would be targeted under the 'foreign power' standard (which cannot be applied to individuals), it is possible that entities could be targeted under certain of the 'agent of a foreign power' standards"). In *United States v. Rahman*, 861 F. Supp. 247, 251 (S.D.N.Y. 1994), one of the defendants claimed that only an "international organization" could be an agent of a foreign power. As the court pointed out, that claim flies in the face of the plain language of the statute, which refers to both "person[s]" and "members" of groups.

FISA actually contains two sets of definitions of the term "agent of a foreign power." The first set, in 50 U.S.C. § 1801(b)(1)(A)-(C), applies to "any person other than a United States person" and therefore does not extend to persons or entities that satisfy the definition of "United States person" in 50 U.S.C. § 1801(i). (A U.S. person includes a citizen of the United States and a lawful permanent resident alien – i.e., a person who has been issued Form I-551. See 8 C.F.R. § 264.1). This first set of definitions does not require the government to establish any criminal conduct by the putative agent of a foreign power. The second set of definitions, in 50 U.S.C. § 1801(b)(2)(A)-(E), applies to "any person," including a U.S. person. These definitions require a stronger showing that the target is acting on behalf of a foreign power, and some showing that his activities violate or may violate criminal law.

[10] This amendment was made by the Intelligence Reform and Preventing Terrorism Act of 2004, Pub. L. 109-177, 120 Stat. 192 (2004), and is now codified at 50 U.S.C. § 1801(b)(1)(C).

[11] See *In re Sealed Case*, 310 F.3d 717, 723 n.9 (FISCR 2002).

[12] 50 U.S.C. § 1801(e)(1).

[13] 50 U.S.C. § 1801(e)(2).

[14] FISA House Report at 47.

[15] *Id.*

[16] *Id.*

[17] FISA House Report at 48 (emphasis added); see also H.R. Rep. No. 98-738, at 17-18 (1984) [hereinafter FISA House Five Year Report] (allowing indexing and logging of acquired communications of U.S. persons if they "reasonably appear" to be foreign intelligence information"). Under the declassified version of the standard minimization procedures in effect as of 1984, information was to be retained if it "reasonably appear[ed]" to be foreign intelligence information. See *id.*

[18] See FISA House Report at 58 (when government is wiretapping a known spy, it is "'necessary' to acquire, retain, and disseminate information concerning all his contacts and acquaintances and his movements").

[19] The information normally will be "concerning" a non-U.S. person because Section 401(a) applies only to non-U.S. person FISA targets, and the target is generally the person from whom, or about whom, information is sought. See FISA House Report at 73.

[20] 50 U.S.C. § 1803(a).

[21] 50 U.S.C. § 1804(a).

[22] 50 U.S.C. § 1805(a).

[23] Under current law, there are four situations in which electronic surveillance may be conducted without advance judicial approval: Under 50 U.S.C. § 1802; in an emergency situation under 50 U.S.C. § 1805(f); for training and testing under 50 U.S.C. § 1805(g); and immediately following a declaration of war by Congress under 50 U.S.C. § 1811.

[24] 50 U.S.C. § 1806(c).

[25] 50 U.S.C. §§ 1807-1808.

[26] 50 U.S.C. § 1809 (criminal liability); see 50 U.S.C. § 1810 (civil liability).

[27] 50 U.S.C. §§ 1801-1811.

[28] 50 U.S.C. § 1801(f)(1)-(4). The definition is unchanged from its enactment in 1978, except that the exclusion in subsection (2) for trespassers as defined in 18 U.S.C. § 2511(2)(i) was added by Section 217 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

[29] 18 U.S.C. §§ 2510-2522.

[30] Subsections (1) and (2) of the definition apply to wire communications.

[31] Subsections (1) and (3) of the definition apply to radio communications.

[32] Subsection (4) of the definition applies to information that is neither a wire nor a radio communication.

[33] See Webster's Revised Unabridged Dictionary 287 (1913).

[34] Although FISA was enacted before the advent of commercially available e-mail, its legislative history makes clear that the statute "is not limited to the acquisition of the oral or verbal contents of a wire communication. It includes the acquisition of any other contents of the communication, for example, where computerized data is transmitted by wire." FISA House Report at 51. The FBI has revealed, in publicly available documents, that it has used FISA for "the interception of telephone and fax communications, and interception of e-mails." Affidavit of FBI Special Agent Randall Thomas, FBI, in support of application for complaint and arrest warrant for James J. Smith (available at http://news.findlaw.com/hdocs/docs/fbi/usleung403cmp.pdf).

[35] Compare 50 U.S.C. § 1801(f)(1)-(3), with 50 U.S.C. § 1801(f)(4). Cf. *Joao v. Sleepy Hollow Bank*, 348 F. Supp. 2d 120, 127 (S.D.N.Y. 2004) (discussing the term "communication device").

[36] Cf., e.g., *United States v. O'Brien*, 391 U.S. 367 (1968) (First Amendment symbolic speech analysis of burning a draft card).

[37] 50 U.S.C. § 1801(l).

[38] FISA House Report at 66.

[39] A possible argument against that conclusion would be to assert that the radio connection between a cordless or mobile handset and a base station or tower is a "like connection" – i.e., like a connection by wire – within the meaning of 50 U.S.C. § 1801(f)(1). However, the legislative history provides explicitly that "[a] radio signal is not within the term, a 'like connection,' in this definition," FISA House Report at 67, and it would be difficult to distinguish on these grounds the radio signal used by a cordless or mobile phone from all other radio signals (other distinctions, such as the use of encryption, would not be directly relevant to the question). Indeed, although commercial cordless and mobile telephones did not exist when FISA was enacted, the legislative history refers to a 1978 analogue: "ordinary marine band [radio] communications, which do not have a reasonable expectation of privacy or require a warrant for law enforcement interception, can be 'patched in' to telephone systems, becoming a 'wire communication.'" FISA House Report at 66. (This portion of the legislative history is actually a discussion of Title III, but the implication is that the marine radio telephone call would be a "wire communication" under FISA only insofar as it was "patched in" and traveling over the telephone system, but not while traveling between the marine radio and the point of reception that connects to the wired telephone system.)

[40] See FISA House Report at 52 (explaining that electronic surveillance of "radio communications" includes "not only the acquisition of communications made wholly by radio but also the acquisition of communications which are carried in part by wire and in part by radio, where the radio transmitted portion of those communications is intercepted"); S. Rep. No. 95-604 at 33. (1977) [hereinafter FISA Senate Judiciary Report].

[41] 18 U.S.C. § 2510(1).

[42] FISA House Report at 66 (contrasting FISA with Title III on this issue). But cf. H. R. Rep. No. 99-647 (1968), at 34 (noting that Title III's "definitions of wire communication and oral communication are not mutually exclusive. Accordingly, different aspects of the same communication might be differently characterized. For example, a person who overhears one end of a telephone conversation by listening in on the oral utterances of one of the parties is intercepting an oral communication. If the eavesdropper instead taps into the telephone wire, he is intercepting a wire communication."). An "electronic communication" as defined by Title III may also travel by wire, but is not thereby rendered a "wire communication."

[43] 50 U.S.C. § 1801(l).

[44] Even after *United States v. Lopez*, 514 U.S. 549 (1995), and its progeny, Congress probably enjoys authority to regulate purely intrastate use of an interstate telecommunications facility. See, e.g., *Weiss v. United States*, 308 U.S. 321, 327 (1939) ("Congress has power, when necessary for the protection of interstate commerce, to regulate intrastate transactions."); see also S. Rep. No. 90-1097 at 92 (1968) (Senate report underlying Title III).

[45] FISA House Report at 66.

[46] Black's Law Dictionary at 87 (8th ed. 2004).

[47] 47 U.S.C. § 153(10); see 47 C.F.R. § 21.2; *National Association of Regulatory Utility Commissioners v. FCC*, 525 F.2d 630 (D.C. Cir. 1976); *Local Exchange Carriers' Rates, Terms & Conditions, for Expanded Interconnection*, 12 FCC Rcd 18730, ¶ 17 (1997); see generally *FCC v. Midwest Video Corp.*, 440 U.S. 689, 701 (1979) (defining a common carrier as an entity that "makes a public offering to provide [communications facilities] whereby all members of the public who choose to employ such facilities may communicate or transmit intelligence of their own design and choosing" (internal quotation marks and citations omitted)). As explained in the text, Title III cross-references the statutory definition in the Communications Act. 18 U.S.C. § 2510(10).

[48] Although Title III defines the term "communication common carrier," the definition no longer plays a significant part in Title III's statutory scheme. It is not part of Title III's definitions of "wire communication," see 18 U.S.C. § 2510(1), or "electronic communication," see 18 U.S.C. § 2510(12). As amended in 1970, Title III required a "communication common carrier" to assist the government in implementing a Title III court order under certain circumstances. See *Dalia v. United States*, 441 U.S. 238, 270 n.19 (1979) (Stevens, J., dissenting). However, following amendments made in 1986 (by ECPA), Title III today requires assistance from a "provider of wire or electronic communication service." 18 U.S.C. § 2518(4); see *In re Application of the U.S. for an Order Authorizing the Roving Interception of Oral Communications*, 349 F.3d 1132, 1136-1137 & n.8, 1139 & n.13 (9th Cir. 2003). "By amending the statute, Congress undeniably intended to expand the scope of the provision to cover more than common carriers." *Id.* at 1139 n.13. The changes to Title III may suggest the need for an amendment to FISA's definition of "wire communication" if the government's proposal does not pass; FISA secondary electronic surveillance orders can be issued not only to a "common carrier," but also to any "other specified person." 50 U.S.C. § 1805(c)(2)(B); cf. *In re Application of the U.S.*, 349 F.3d at 1141-1143 (discussing "other person" as used in Title III).

[49] The 1978 House Report on FISA explains that "one of the committee's purposes has been to produce legislation that can be read and understood (and thus complied with) easily, without excessive cross reference to other statutes." FISA House Report at 98. To the extent that FISA requires cross-reference to the Communications Act with respect to the meaning of "common carrier," it tends to frustrate that purpose.

[50] See, e.g., *National Communications Ass'n, Inc. v. A.T.&T Corp.*, 238 F.3d 124, 125 (2d Cir. 2001).

[51] See 47 U.S.C. § 332(c)(1)(A).

[52] 47 U.S.C. § 541(c). For the FCC's definition of a "cable television system," see 47 C.F.R. § 76.5; see also 47 U.S.C. § 522(7). The definition of "wire communication" in FISA includes signals while being carried by a "cable" as well as a "wire." 50 U.S.C. § 1801(l).

[53] The FCC has not yet determined whether providers of VOIP are common carriers under the Communications Act. See IP-Enabled Services, Notice of Proposed Rulemaking, 19 FCC Rcd 4863, ¶ 43 (2004) (regarding VoIP). The FCC explains that "VoIP allows you to make telephone calls using a computer network, over a data network like the Internet. VoIP converts the voice signal from your telephone into a digital signal that travels over the internet then converts it back at the other end so you can speak to anyone with a regular phone number. When placing a VoIP call using a phone with an adapter, you'll hear a dial tone and dial just as you always have. VoIP may also allow you to make a call directly from a computer using a conventional telephone or a microphone." See www.fcc.gov/voip/. However, interpreting and applying the Communications Assistance to Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001-1021, the FCC has publicly mandated that VOIP providers configure their systems to

aid wiretapping by the federal government. www.fcc.gov.wcb/iatd/calea.html. For a discussion of this mandate by (among others) a former NSA official, see http://itaa.org/news/docs/CALEAVOIPreport.pdf.

[54] *NCTA v. Brand X Internet Services*, 545 U.S. 967 (2005). "Shortly after the *Brand X* decision, the FCC convened its Open Commission Meeting on August 5, 2005, and adopted a policy that both DSL and cable modem services are information services and not subject to common carrier regulation." Anna Zichterman, Note, *Developments In Regulating High-Speed Internet Access: Cable Modems, DSL, & Citywide Wi-Fi*, 21 Berk. T. LJ 593, 604 (2006) (citing *In re Appropriate Framework for Broadband Access to the Internet over Wireline Facilities*, 20 F.C.C.R. 14853, 14871-72 (2005) (available at http://hraunfoss.fcc.gov/edocs_ public/attachmatch/FCC-05-150A1.pdf); Press Release, FCC Eliminates Mandated Sharing Requirement on Incumbents' Wireline Broadband Internet Access Services (Aug. 5, 2005) (available at http:// hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-260433A1.pdf)).

[55] See, e.g., *Howard v. America Online, Inc.*, 208 F.3d 741, 752-753 (9th Cir. 2000).

[56] See *Brand X*, 545 U.S. at 973-974.

[57] For NASA's description of wavelengths and the electromagnetic spectrum (targeted at students in grades 5-8, but also within the grasp of most lawyers), see www.nasa.gov/audience/forstudents/5-8/features/F_The_Electromagnetic_Spectrum.html.

[58] See FISA House Report at 52 (referring to a ham radio or CB signal).

[59] See *id.* at 52 ("It is the committee's intent that the intentional acquisition of the contents of a communication being transmitted by common carrier radio microwave ... would clearly be included here"), 67 ("Interception of microwave communications carried by common carriers, by intercepting the radio signal, is electronic surveillance").

[60] However, the FCC explains that microwaves are "in the upper range of the radio spectrum." See http://wireless.fcc.gov/microwave/.

[61] FISA House Report at 52. See *United States v. Karo*, 468 U.S. 705 (1984). In some situations, there is no reasonable expectation of privacy in the location of an object or vehicle – e.g., when a vehicle is on the open road and subject to physical surveillance. But information about location is a type of information that may be acquired via "electronic surveillance," depending on the circumstances. Where a radio communication is unintentionally acquired, it generally must be destroyed. See 50 U.S.C. § 1806(i).

[62] Under 50 U.S.C. § 1801(f)(3), concerning radio communications, the acquisition must be "[i]ntentional." The legislative history explains that "by their very nature, radio transmissions may be intercepted anywhere in the world, even though the sender and all intended recipients are in the United States [an element of "electronic surveillance" as defined by Subsection (3)]. Thus, intelligence collection may be targeted against foreign or international communications but accidentally and unintentionally acquire the contents of [radio] communications intended to be totally domestic." FISA House Report at 52. By negative implication, this suggests that accidental acquisition may qualify as "acquisition" under the remaining three subsections of current 50 U.S.C. § 1801(f).

[63] While FISA uses the term "acquisition" and Title III uses the term "interception" to describe surveillance, the latter statute defines "interception" as "the aural or other *acquisition* of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). Perhaps for that reason, FISA's legislative history sometimes uses the terms interchangeably. See, e.g., House Report at 55 ("By minimizing acquisition, the committee envisions, for example, that in a given case, where *A* is the target of the wiretap, after determining that *A*'s wife is not engaged with him in clandestine intelligence activities, the interception of her calls on the tapped phone, to which *A* was not a party, probably ought to be discontinued as soon as it is realized that she rather than *A* was the party").

[64] See *George v. Carusone*, 849 F. Supp. 159, 163 (D. Conn. 1994); see also *United States v. Lewis*, 406 F.3d 11, 17 n.5 (1st Cir. 2005); cf. *United States v. Hammoud*, 286 F.3d 189, 192-193 (4th Cir. 2002). The Ninth Circuit

appears to have held that the routine recording of incoming calls by a sheriff's office is not "interception" under Title III because it does not involve "active surveillance." *Greenfield v. Kootenai County*, 752 F.2d 1387 (9th Cir. 1985). Whatever the merits of Greenfield's reasoning with respect to Title III, it seems dubious as applied to FISA. Cf. *Ariasi v. Mutual Central Alarm Service, Inc.*, 202 F.3d 553, 557-558 (2d Cir. 2000) (noting that "[t]he case law with respect to Title III is somewhat unclear regarding the proper definition of an 'interception' under the statute" and citing and discussing cases).

[65] See, e.g., Glenn A. Fine, Department of Justice Inspector General, *Top Management Challenges in the Department of Justice* (2004) (noting that "the FBI's collection of material requiring translation outpaced its translation capabilities and the FBI did not translate all the foreign language counterterrorism and counterintelligence material it collected," and that "the FBI's digital collection systems have limited storage capacity and consequently unreviewed audio sessions are sometimes deleted automatically to make room for incoming audio sessions") (available at www.usdoj.gov/oig/challenges/2004.htm).

[66] See Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, FBI, Before the United States Senate Committee on the Judiciary (Sept. 6, 2000) (available at www.fbi.gov/congress/congress00/kerr090600.htm).

[67] *Id.*

[68] That accords with FISA's use of "acquisition" in the definition of "minimization procedures." 50 U.S.C. § 1801(h)(1). Under Defense Department regulations, information is "collected" when it has been "received for use by an employee of a DoD intelligence component," and "[d]ata acquired by electronic means is 'collected' only when it has been processed into intelligible form." Department of Defense, DOD 5240 1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons* § C.2.2.1 (Dec. 1982) (available at www.dtic.mil/whs/directives/corres/text/d52401p.txt) [hereinafter DOD 5240 1-R]; see also National Security Agency, United States Signals Intelligence Directive 18 § 9.2 (July 1993) (available at www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm) [hereinafter USSID-18].

[69] This phrase appears in all four subsections of current 50 U.S.C. § 1801(f).

[70] 18 U.S.C. § 2510(5).

[71] See 18 U.S.C. § 2511.

[72] 50 U.S.C. §§ 1809, 1810.

[73] FISA House Report at 53.

[74] *United States v. Dubrofsky*, 582 F.2d 208, 211 (9th Cir. 1978) (holding that these techniques are not "searches" within the meaning of the Fourth Amendment). See *United States v. Place*, 462 U.S. 696, 707 (1983) (holding that a dog sniff is not a Fourth Amendment "search").

[75] Compare *Kyllo v. United States*, 533 U.S. 27 (2001) (use of sense-enhancing technology to gather information regarding the interior of a home that could not otherwise have been obtained without a physical intrusion into a constitutionally protected area constitutes a "search" for Fourth Amendment purposes), with, e.g., *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (aerial photography of a business not a Fourth Amendment "search").

[76] Cf. *Kyllo*, 533 U.S. at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search – at least where (as here) the technology in question is not in general public use" (citations omitted)).

[77] 18 U.S.C. § 2512(1)(b) (prescribing punishment for anyone who "manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it

primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce").

[78] The cases are collected in Tammy Hinshaw, *What Constitutes "Device Which Is Primarily Useful for the Surreptitious Interception of Wire, Oral, or Electronic Communication," Under 18 U.S.C.A. § 2512(1)(B), Prohibiting Manufacture, Possession, Assembly, Sale of Such Device*, 129 A.L.R. Fed. 549 (2004).

[79] See, e.g., *United States v. Schweihs*, 569 F.2d 965 (5th Cir. 1978).

[80] See S. Rep. No. 90-1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2183-84 ("The prohibition will thus be applicable to, among others, such objectionable devices as the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack.").

[81] 50 U.S.C. § 1801(n).

[82] 18 U.S.C. § 2510(8) ("'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication").

[83] Thus, it includes the information acquired by pen/trap surveillance. Section 401(e) of the government's proposal would change the definition of "contents" in FISA.

[84] See FISA House Report at 67.

[85] 50 U.S.C. § 1801(f)(2), (4).

[86] 50 U.S.C. § 1801(j).

[87] Cf. *Rasul v. Bush*, 124 S. Ct. 2686, 2696 (2004).

[88] FISA House Report at 65.

[89] *Salisbury v. United States*, 690 F.2d 966, 968-969 (D.C. Cir. 1982) (citations omitted, ellipsis in original). As described here, the technology used in NSA watchlisting is different from the technology used in the FBI's Carnivore system. While NSA intercepted all communications on a monitored channel, and then later discarded any intercepted communications that were not responsive to a watch list, Carnivore effectively combines the two steps, capturing communications in a computer's random access memory and discarding them before they are recorded to a hard drive or other permanent media if they do not meet the criteria established by the device's programming. For a more complete discussion of watchlisting and FISA, see House FISA Five Year Report at 5-6.

[90] See, e.g., *Ring v. Arizona*, 536 U.S. 584, 620 & n.1 (2002) (O'Connor, J., dissenting) (referring to a Westlaw search); *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003) (vacating discovery order allowing tort plaintiff unlimited access to Ford's databases without designating search terms to restrict the search).

[91] FISA House Report at 51 (emphasis added). One rationale for this may have been to avoid civil liability for accidental interceptions. Cf. FISA Senate Judiciary Report at 33-34 (discussing use of "intentional" standard in Subsection (3) of the current definition of "electronic surveillance").

[92] 50 U.S.C. § 1801(j).

[93] Subsection (2) of the current definition of "electronic surveillance" applies only when no party to the communication has consented to the surveillance.

[94] 389 U.S. 347, 360-362 (1967).

[95] See, e.g., *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).

[96] FISA House Report at 54.

[97] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 272-273 (1990). In his dissenting opinion in *Verdugo-Urquidez*, Justice Brennan stated that "[n]umerous lower courts ... have held that illegal aliens in the United States are protected by the Fourth Amendment, and not a single lower court has held to the contrary." *Id.* at 283 n.6 (Brennan, J., dissenting) (citing cases).

[98] FISA House Report at 54.

[99] 50 U.S.C. § 1801(f)(1), (3), (4) (emphasis added).

[100] Subsection (1) of the current definition refers to acquisition of a communication sent to or from "a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." Subsection (2) of the current definition refers to acquisition of the contents of any wire communication "to or from a person in the United States, without the consent of any party thereto." Current Subsection (3) refers to intentional acquisition of a communication "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States." And current Subsection (4) refers to acquiring information "under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(1)-(4). Had Congress intended a narrower approach, the more natural phrasing would have been "that person" (i.e., the targeted person), in Subsection (1), "a party" to the communication in Subsection (2), "the sender and all intended recipients" of the communication in Subsection (3), and "the target" of the surveillance in Subsection (4).

[101] 50 U.S.C. § 1821(5).

[102] See 50 U.S.C. § 1822(c) (FISC has jurisdiction to issue orders authorizing physical searches).

[103] See *Minnesota v. Carter*, 525 U.S. 83 (1998); cf. *Steagald v. United States*, 451 U.S. 204 (1981) (absent consent or exigent circumstances, government may not search for the subject of an arrest warrant in the home of a third party without a search warrant for the third party's home). See generally *Stanford Daily v. Zurcher*, 436 U.S. 547 (1978) (upholding warrants directed at third parties who possess evidence of a defendant's crime). Even if the defendant in a criminal case cannot invoke the exclusionary rule in such a case – because he individually lacks a reasonable expectation of privacy – the existence of a reasonable expectation of privacy held by any person in the place to be searched requires adherence to Fourth Amendment requirements. Similarly, under current Subsections (1), (3), and (4), and the current definition of "physical search," a FISC order is normally required where a search or surveillance would infringe on any person's reasonable expectation of privacy (and the other elements of the definitions and the statute are met).

[104] FISA House Report at 53.

[105] *Id.*

[106] *Id.*

[107] *Id.*

[108] See FISC R. 10(A)(i) (available at www.uscourts.gov/rules/FISC_Final_Rules_Feb_2006.pdf).

[109] The analogous element in current Subsection (2) is "the consent of any party" to an intercepted communication.

[110] *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973).

[111] *United States v. Robinson*, 414 U.S. 218 (1973); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (allowing search incident to arrest of a pager because pager data is transient).

[112] *Carroll v. United States*, 267 U.S. 132 (1925).

[113] *South Dakota v. Opperman*, 428 U.S. 364 (1976).

[114] As discussed elsewhere in these comments, an e-mail user may have no reasonable expectation of privacy in an e-mail sent through his ISP, but if the ISP is an "electronic communications service" as defined by Title III and Chapter 206 of Title 18, the government will need a warrant to compel production of the e-mail if it is less than six months old and has not yet been read. Under 18 U.S.C. § 2703(a), "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant."

[115] There is no reasonable expectation of privacy in the "routing and addressing" information obtained by pen/trap surveillance (at least when obtained from a third party), see *Smith v. Maryland*, 442 U.S. 735 (1979), but the government cannot get such information for law enforcement purposes without a pen/trap order from a district court. A pen/trap order may not be a "warrant" within the meaning of 50 U.S.C. § 1801(f), however, because it does not require a showing of probable cause. Either way, pen/trap surveillance of wire communications, conducted in the United States, of any person in the United States, is "electronic surveillance" under current FISA absent consent, because current Subsection (2) does not depend on the existence of a reasonable expectation of privacy or the need for a warrant. See 50 U.S.C. § 1801(f)(2).

[116] Pub. L. 107-56, § 1003, 115 Stat. 272, 392 (Oct. 26, 2001).

[117] Section 2511(2)(i) provides:

> It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if –
>
> (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
>
> (II) the person acting under color of law is lawfully engaged in an investigation;
>
> (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and
>
> (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.
>
> The term "protected computer" means a computer –
>
> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

18 U.S.C. § 2510(20) and 18 U.S.C. § 1030(e)(2).

The term "computer trespasser" –

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer.

18 U.S.C. § 2510(21).

[118] This provision is limited to such communications as defined by Title III, not FISA.

[119] In some cases, a hacked computer is used as a pass-through to reach a third computer that the hacker is exploiting, the owner of the pass-through computer probably would not be a "party" to the hacker's communication with the third, exploited computer, and so the provision could make a difference.

[120] To the extent that they are exempt from regulation under FISA, such communications are also exempt from regulation under Title III. A provision of Title III provides specifically that "[n]othing contained in this chapter [18 U.S.C. §§ 2510-2522] or chapter 121 [the Stored Communications Act, 18 U.S.C. §§ 2701-2712] or 206 [the pen/trap provisions of 18 U.S.C. §§ 3121-3127] of this title, or section 705 of the Communications Act of 1934 [47 U.S.C. § 605], shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f). See also 50 U.S.C. § 1821(5) (similar exemption in FISA's current definition of "physical search").

[121] Current Subsection (1) applies only to wire and radio communications involving "a particular, known United States person who is in the United States." Subsection (2) applies only to wire communications "to or from a person in the United States." Subsection (3) applies only to radio communications "if both the sender and all intended recipients are located within the United States." 50 U.S.C. § 1801(f)(1)-(3).

[122] Current Subsection (4) requires the "installation or use" of a surveillance device "in the United States." If one or more of the parties to a communication were standing just outside the U.S. border, and the government used a boom microphone to record at least one side of the communication from just inside the border, it would be "electronic surveillance" under current Subsection (4) because the surveillance device – the microphone – would be used inside the U.S.

[123] Nor would Title III apply in that situation. See, e.g., *United States v. Barona*, 56 F.3d 1087, 1090 (9th Cir. 1995) ("When determining the validity of a foreign wiretap, we start with two general and undisputed propositions. The first is that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-21, 'has no extraterritorial force'"); *United States v. Peterson*, 812 F.2d 486, 492 (9th Cir. 1987) (citing cases for the proposition that Title III has no extraterritorial application); see generally, e.g., *EEOC v. Arab American Oil Co.*, 499 U.S. 244 (1991) (general presumption against extraterritorial application of U.S. statutes). In general, no U.S. court can issue an ordinary search warrant for a foreign jurisdiction. See *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).

[124] FISA House Report at 51.

[125] Cf. 18 U.S.C. § 2511(2)(g) ("It shall not be unlawful under this chapter or chapter 121 of this title for any person – (i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public; (ii) to intercept any radio communication which is transmitted – (I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system").

[126] Cf. *United States v. Smith*, 978 F.2d 171, 179 (5th Cir. 1992) ("cordless phones now appearing on the market actually scramble the radio signal so that even radio scanners cannot intercept the communication").

[127] 50 U.S.C. § 1822(c).

[128] 50 U.S.C. § 1823.

[129] 50 U.S.C. § 1824.

[130] 50 U.S.C. § 1822(a).

[131] 50 U.S.C. § 1825.

[132] 50 U.S.C. § 1826.

[133] 50 U.S.C. §§ 1827 (criminal liability), 1828 (civil liability).

[134] Under 50 U.S.C § 1821(1), the term "United States" has the same meaning in the context of a physical search as it does in the context of electronic surveillance.

[135] 533 U.S. 27 (2001).

[136] As the Court explained in *Kyllo*, "[t]hermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth – black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images." *Id.* at 29-30.

[137] *Id.* at 30.

[138] *Id.* at 31.

[139] *Id.* at 31-32 (internal quotations omitted).

[140] *Id.* at 33.

[141] *Id.* at 34 (internal quotations and citation omitted).

[142] *Id.* at 32 n.1 (quoting N. Webster, *An American Dictionary of the English Language* 66 (1828)).

[143] *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (footnote omitted).

[144] H.R. Conf. Rep. No. 103-753 at 80 (1994) [hereinafter FISA Search Conference Report].

[145] 50 U.S.C. § 1801(f)(4).

[146] 18 U.S.C. § 2511(2)(f) ("Nothing contained in this chapter ... shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications ... utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978").

[147] FISA House Report at 100. As the Senate Judiciary Report underlying FISA went on to explain, citing to the Church Committee reports on abuses by the government, "[t]he activities of the National Security Agency pose particularly difficult conceptual and technical problems which are not dealt with in this legislation." S. Rep. No. 95-604 at 64 (1977).

[148] In 1986, Congress concluded that there is no reasonable expectation of privacy in cordless telephone calls because the radio signals broadcast by such telephones can be intercepted easily, and therefore exempted their interception from regulation under Title III. Electronic Communications Privacy Act (ECPA), Pub. L. No. 508, 99th Cong., 2d Sess., § 101(a)(1)(D), 100 Stat. 1848 (1986) (adding the following to the definition of "wire communication" in Title III: "such term does not include the radio portion of a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit"). As the Senate Report underlying ECPA explained, "[b]ecause communications made on some cordless telephones can be intercepted easily with readily available technologies, such as an AM radio, it would be inappropriate to make the interception of such a communication a criminal offense." S. Rep. No. 99-541 at I2 (1986). In 1994, however, Congress eliminated the exemption, bringing cordless telephone transmissions within the scope of Title III. See Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 414, 103rd Cong., 2d Sess. § 202(a), 108 Stat. 4279 (1994) (deleting the language added by ECPA). As the House Report underlying CALEA explained, a privacy and technology task force examined "the newer generation of cordless phones" and recommended that "the legal protections of ECPA be extended" to cover them; the task force found that "'[t]he cordless phone, far from being a novelty item used only at 'poolside,' has become ubiquitous ... More and more communications are being carried out by people [using cordless phones] in private, in their homes and offices, with an expectation that such calls are just like any other phone call.' Therefore, [CALEA] includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority." H.R. Rep. No. 103-827 at 12, 17 (1994) (last ellipsis in original).

The courts of appeals have not authoritatively resolved the reasonableness of an expectation of privacy in the radio signal emitted by cordless telephones. See, e.g., *Frieerson v. Goetz*, 99 Fed. Appx. 649, 2004 WL 1152172 (6th Cir. May 19, 2004) (unpublished decision) (granting qualified immunity for unauthorized interception of cordless telephone radio signal). However, it may be that expectations of privacy in newer generations of cordless telephones, used after CALEA, will be found to be reasonable, even if that is not the case for older models used before CALEA. See, e.g., *Price v. Turner*, 260 F.3d 1144, 1148 (9th Cir. 2001) ("At the time of Price's cordless phone conversations [1989-1991], they were readily susceptible to interception. For that very reason, the transmissions were not protected by the Wiretap Act. Price cannot be said to have had an objectively reasonable expectation of privacy in those communications"); *United States v. Smith*, 978 F.2d 171, 180 (5th Cir. 1992) ("as technological advances make cordless communications more private at some point such communication will be entitled to Fourth Amendment protection. Given this conclusion, it should be equally obvious that it is not enough for a trial court to conclude that interception of a conversation does not implicate Fourth Amendment concerns simply because it is carried by a 'cordless' phone. Application of the Fourth Amendment in a given case will depend largely upon the specific technology used").

[149] See, e.g., *Katz v. United States*, 389 U.S. 347 (1967); 18 U.S.C. §§ 2510-2522.

[150] FISA House Report at 50 (emphasis in original).

[151] Thus, for example, the kind of surveillance alleged to have taken place in *Blind Man's Bluff*, in which the U.S. Navy tapped an undersea telephone cable used to carry communications between Soviet military officials outside the United States, would not be regulated by FISA. Sherry Sontag & Christopher Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage* (Harper 1998).

[152] One argument against this conclusion is that acquisition of the contents of a radio communication is electronic surveillance under subsection (3) if the "sender and all intended recipients" of the radio communication itself are in the United States. On that argument, the "recipient" of the radio communication is the cordless telephone's base station; the other human party to the telephone call is the recipient only of the (international) wire communication that begins after the (domestic) radio communication arrives at the cordless telephone base station. This argument, however, seems quite strained. When FISA was enacted in 1978, as discussed in the text, the radio portions of international telephone calls (made by non-U.S. persons) were exempt from regulation. See FISA Senate Judiciary Report at 34.

[153] Under 18 U.S.C. § 2510(1) and (12), a "wire communication" is an "aural" transfer, and an "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature" other than a wire or oral communication. A fax is an "electronic communication" under Title III.

[154] One difference is that a fax, unlike a telephone call, generates a permanent record of its contents – the paper that comes out of the recipient's fax machine. Acquisition of the contents of this paper after it has been removed from the fax machine would be treated like the acquisition of any other paper under FISA. The fact that it had been sent by fax would be irrelevant if the acquisition occurred after it was out of the fax machine.

[155] For example, the Global System for Mobile Communications (GSM) protocol is generally used in Europe (and elsewhere).

[156] Instead, they would be regulated by Section 2.5 of Executive Order 12333.

[157] The basics of e-mail and voice mail protocols, and the ways in which they differ from traditional telephone protocols, are not too difficult to grasp. Here is how the government described e-mail in a brief filed in the First Circuit in November 2004:

> e-mail is an electronic transfer of a message from one computer user to another. An e-mail message typically travels through a series of computers as it goes from sender to receiver. The sender creates the e-mail message using an e-mail program and directs the program to send the message. Once sent, the message travels from the sender's computer to the sender's e-mail service provider. The provider's computer accepts the message using a program called a "Message Transfer Agent" (MTA), saving the message to either the computer's random access memory (RAM) or its hard drive. The MTA forwards the accepted message out through the Internet to yet another computer, which then repeats the process of using an MTA to accept and forward the message to another computer, and so on. This process of passing a message from computer to computer is known as the "store-and-forward" process. The computer-to-computer transmission continues until the MTA at the recipient's e-mail service provider accepts the message and stores it in a location accessible to the recipient, that is, his inbox. This is known as "final delivery," and is often achieved with the assistance of a program called a "Message Delivery Agent" (MDA).

Supplemental Brief for the United States, *United States v. Councilman*, No. 03-1383 (1st Cir. Nov. 4, 2004), 2004 WL 3201458. For a more complete discussion of e-mail and the Internet, see http://computer.howstuffworks.com/email.htm.

As this excerpt reveals, there is an argument that an e-mail message consists of not one, but several discrete "communications." At the most basic level, ignoring the actual complexity of the Internet, the first communication would be between the sender and his own ISP, the next would be between the sender's ISP and the recipient's ISP (or any intermediate computers), and the last would be between the recipient's ISP and the recipient as he downloads the e-mail onto his personal computer. That is not, however, how the courts have analyzed e-mail communications under criminal law surveillance provisions. See *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (en banc) ("We conclude that the term 'electronic communication' [as used in Title III] includes transient electronic storage that is intrinsic to the communication process for such communications").

[158] As the First Circuit explained in *Councilman*:

> There are at least five discrete stages at which an electronic mail message could be intercepted and its contents divulged to an unintended receiver: at the terminal or in the electronic files of the sender, while being communicated, in the electronic mailbox of the receiver, when printed into hardcopy, and when retained in the files of the electronic mail company for administrative purposes.

418 F.3d at 76 (quoting Office of Technology Assessment, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* (available at www.wws.princeton.edu/ ota/disk2/1985/8509_ n.html (Oct.1985))).

[159] For a discussion of POTS, see http://electronics.howstuffworks.com/telephone.htm.

[160] By contrast, a traditional telephone call does not leave footprints of its content in the telecommunications network. There is no content to be acquired either before the parties to a call connect, or after they hang up. Thus, electronic surveillance of such a telephone call is possible, if at all, only in real time, when the call is either a wire or radio communication. That is how the courts of appeals have interpreted the corresponding provisions in Title III. See, e.g., *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2004) ("every circuit court to have considered the matter has held that an 'intercept' under the ECPA must occur contemporaneously with transmission of the electronic communication"); *United States v. Steiger*, 318 F.3d 1039, 1048-1049 (11th Cir. 2003) ("a contemporaneous interception – i.e., an acquisition during 'flight' – is required to implicate the Wiretap Act with respect to electronic communications"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 459-460 (5th Cir. 1994).

[161] Voice mails are entrusted to and stored by third parties only if stored by the telephone company as part of a voice-mail service, not if they are simply recorded on a stand-alone home answering machine.

[162] 50 U.S.C. § 1801(l).

[163] That would be the case unless an ISP's e-mail server were treated as a "wire" that is "carry[ing]" the e-mail it stores, which seems implausible.

[164] 50 U.S.C. § 1801(f)(1)-(3).

[165] 50 U.S.C. § 1801(f)(4).

[166] Similarly, acquisition of stored communications from a target's personal computer, or his home answering machine, could also involve a "surveillance device," again depending on the facts. If a government agent simply enters a target's home and listens to his voice mail, or copies e-mail from his personal computer's hard drive to a CD or other portable storage media, it probably would not qualify as "electronic surveillance" under Subsection (4) because the acquisition does not involve a "device," as discussed above. (It could, however, qualify as a "physical search.") However, a concealed microphone that overhears a voice mail being played by the target, or a concealed video camera that records a computer screen while an e-mail is displayed on it, would be a "surveillance device" under Subsection (4).

[167] 50 U.S.C. § 1821(5) provides that a physical search "does not include ... 'electronic surveillance', as defined in section 1801(f)." Thus, acquisition of stored communications can be a "physical search" only if it has been found not to be "electronic surveillance." The distinction between treating acquisition of stored communications as a search rather than surveillance may have little impact on civil liberties, but it may be significant to certain members of the Intelligence Community – for example, under the publicly available version of Executive Order 12333, the NSA may conduct electronic surveillance, but may not conduct physical searches, inside the United States.

[168] 50 U.S.C. §§ 1801(f)(4) (electronic surveillance), 1821(5) (physical search).

[169] See *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004).

[170] 18 U.S.C. §§ 2702(a)(1), 2703(a). Ordinarily, information held by third parties is subject to subpoena, and so a warrant might not be necessary. See generally *United States v. R. Enterprises*, 498 U.S. 292 (1991); cf. *Hale v. Henkel*, 201 U.S. 43, 76-77 (1906) (using Fourth Amendment to determine "reasonableness" of a subpoena). By statute, 18 U.S.C. § 2703(b), communications held in storage for more than 180 days may be acquired by warrant or subpoena, among other methods. Thus, acquisition of these older communications is not governed by FISA.

[171] Under 18 U.S.C. § 2510(15), which applies here pursuant to 18 U.S.C. § 2711(1), an "electronic communication service" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." The legislative history explains that "telephone companies and electronic mail companies are providers of electronic communication services." S. Rep. No. 99-541 at 14 (1986).

[172] Under 18 U.S.C. § 2510(17), which applies here pursuant to 18 U.S.C. § 2711(1), the term "electronic storage" means either "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof"; or "(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." The precise meaning of this provision remains uncertain. See *United States v. Councilman*, 418 F.3d 67 (1st Cir. 2005) (en banc). The Department of Justice, which supported rehearing in *Councilman*, acknowledges that "e-mail that has been received by a recipient's service provider but has not yet been accessed by the recipient is in 'electronic storage,'" but maintains that it is not in such storage after "the recipient retrieves the e-mail." DOJ's argument is that retrieved e-mail is "no longer in 'temporary, intermediate storage ... incidental to ... electronic transmission.'" Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Part III.B (July 2002) (available at www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm#_IIIB_).

Whatever the merits of these arguments, it seems clear that unread e-mail less than six months old, held on the server of the sender or recipient's ISP, is in "electronic storage." Such storage will almost always be in an "electronic communications system" because that term is defined broadly to mean "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14) (applicable here pursuant to 18 U.S.C. § 2711(1)). As a practical matter, because the government cannot know in advance when a recipient will retrieve any particular e-mail, and because it obviously prefers to read a suspected terrorist's e-mail before the terrorist himself does so, it must effectively proceed in all cases as if bound by the restrictions.

[173] 442 U.S. 735 (1979). Although *Smith v. Maryland* was decided several months after FISA's enactment, Congress seems to have anticipated its holding, because it understood that pen/trap surveillance would be "electronic surveillance" under 50 U.S.C. § 1801(f)(2), the part of the definition that does not require a reasonable expectation of privacy. See FISA House Report at 51. Under Subsection (2), pen/trap surveillance conducted in real time is "electronic surveillance" where the "acquisition" occurs in the United States (i.e., the surveillance is conducted in the United States), and at least one party to the communication is in the United States, unless a party consents to the surveillance.

[174] *Smith*, 442 U.S. at 743 (citations omitted).

[175] 425 U.S. 435 (1976).

[176] See also *Couch v. United States*, 409 U.S. 322, 335-336 & n.19 (1973) (no reasonable expectation of privacy in financial papers provided to an accountant). Decisions such as *Hoffa v. United States*, 385 U.S. 293, 302 (1966), which upheld the practice of consensual monitoring, should be distinguished because they hold only that any party to a private communication may consent to law enforcement monitoring of the communication. The sender retains a reasonable expectation of privacy in such communications despite the possibility that the recipient may consent, and absent consent a warrant is still required. By contrast, when an otherwise private communication is conveyed and made available to third parties, *Smith* and *Miller* can be read to hold that the reasonable expectation of privacy is simply lost. The Court has not always maintained the distinction, however, perhaps because, as a practical matter, the third party's consent or a warrant or subpoena is usually required for the government to get access to the

information because the third party's reasonable expectation of privacy in the place where the information is being kept. See, e.g., *Miller*, 425 U.S. at 440 (citing Hoffa). This fact is critical under FISA.

[177] 442 U.S. at 743.

[178] *Id.* at 743-744 (citations omitted). In *Miller*, the Court stated that it "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U.S. at 443.

[179] As the Senate Report underlying Chapter 121 explains (S. Rep. No. 99-541 at 3 (1986) (footnote omitted)):

> The Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity. For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection. See *United States v. Miller*, 425 U.S. 435 (1976) (customer has no standing to contest disclosure of his bank records). Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties. The provider of these services can do little under current law to resist unauthorized access to communications.

[180] See 18 U.S.C. § 2702(b)(6) (allowing electronic communications service provider to disclose the contents of a communication to the National Center for Missing and Exploited Children without a warrant or consent). Under 42 U.S.C. § 13032(b)(1), if an electronic communication service provider "obtains knowledge of facts or circumstances from which a violation of [certain criminal statutes] involving child pornography ... is apparent," then it "shall, as soon as reasonably possible, make a report of such facts or circumstances to the Cyber Tip Line at the National Center for Missing and Exploited Children, which shall forward that report to a law enforcement agency or agencies designated by the Attorney General." (Perhaps this provision could be defended based on one of the warrant exceptions to the Fourth Amendment, but it seems unlikely.)

[181] For example, the Court could distinguish *Miller* on the ground that "the documents subpoenaed here are not respondent's 'private papers,'" and perhaps also on the ground that, assuming defendants' own documents were involved, "[t]he checks are not confidential communications but negotiable instruments to be used in commercial transactions." 425 U.S. at 440, 442. The Court could distinguish *Smith* on the ground that it did not involve the "contents" of a communication. Moreover, as commentators have noted, there are reasons to doubt the reasoning of *Miller*. See, e.g., Patricia L. Bellia, *Spyware and the Limits of Surveillance Law*, 20 Berkley Tech. L. J. 1283, 1292 & n.45 (2005) (criticizing *Miller*).

[182] *Miller* rejected a similar argument based on the Bank Secrecy Act.

[183] In *United States v. Maxwell*, 45 M.J. 406, 417 (C.A.A.F.), the Court of Appeals for the Armed Forces held that an AOL account holder had a reasonable expectation of privacy in the e-mails he sent through AOL, in part because "AOL's policy was not to read or disclose subscribers' e-mail to anyone except authorized users, thus offering its own contractual privacy protection in addition to any federal statutory protections."

[184] See, e.g., *Kyllo*, 533 U.S. at 31 (Scalia, J.).

[185] Compare, e.g., *California v. Greenwood*, 486 U.S. 35 (1988) (no reasonable expectation of privacy in garbage left on the curb for pickup by trash collector), with, e.g., *Ex parte Jackson*, 96 U.S. (6 Otto) 727, 733 (1878)

(reasonable expectation of privacy in sealed, first-class mail); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970) (same). Unlike a letter, an e-mail is not sealed, but some ISPs have policies or contractual arrangements under which they do not read or disclose subscribers' e-mails.

[186] The cases in this area are collected in Mitchell Waldman, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5th 15 (2004).

[187] 50 U.S.C. § 1801(f)(4).

[188] See 18 U.S.C. § 2702.

[189] If such acquisition of stored e-mail is a "physical search" (rather than "electronic surveillance") under FISA, however, there may be a question about the intersection with the Stored Communications Act, which (like Title III) generally prohibits disclosure of certain stored communications and also provides for certain exemptions. Under 18 U.S.C. § 2511(2)(e), neither the Stored Communications Act nor any other provision of Title 18 of the U.S. Code makes it "unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act." There is no corresponding exemption, however, for physical searches under FISA. Under 18 U.S.C. § 2511(2)(f), the Stored Communications Act "shall [not] be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978." This could in theory apply to FISA physical searches, because they are a means other than electronic surveillance as defined in FISA, but certainly would not apply to physical searches of a domestic ISP to obtain domestic e-mail messages. This exemption was adopted in 1978 to protect certain signals intelligence activities of the National Security Agency. See FISA House Report at 100.

[190] 18 U.S.C. § 2511(2)(c).

[191] This assumes that "a person" has a reasonable expectation of privacy that is implicated by the circumstances under which the government conducts the surveillance, as would be the case when the government enters the premises of the ISP.

[192] Current Subsection (1) could also apply if the target were a U.S. person, but where – as here – the acquisition of e-mail occurs in the United States, Subsection (2) is effectively broader in scope than Subsection (1). In particular, current Subsection (2) does not depend on the existence of a reasonable expectation of privacy or the need to use a warrant for law enforcement purposes, but only on the absence of consent from a party to the acquired communication (or applicability of the computer-trespasser exception from Title III).

[193] If neither party to the e-mail were located in the United States, then acquisition would not be regulated under current Subsection (2), but acquisition of e-mail to or from a U.S. person abroad would be governed by Section 2.5 of Executive Order 12333.

[194] The executive branch has maintained that the President has inherent authority to conduct electronic surveillance (in the non-technical sense) for national security purposes involving foreign powers or their agents, and could advance the argument that such power cannot be restrained by Congress, at least in certain circumstances.

[195] 18 U.S.C. § 2511(2)(e).

[196] 18 U.S.C. § 2511(2)(f).

[197] FISA House Report at 100.

[198] Letter from Lt. Gen. Keith Alexander, Director, NSA, to Senator Arlen Specter, Chairman, Committee on the Judiciary, U.S. Senate (19 December 2006) (Answer to Question 2a: "When FISA was enacted into law in 1978,

almost all transoceanic communications into and out of the United States were carried by satellite and those communications were, for the most part, intentionally omitted from the scope of FISA"). Subsection (2) of the current definition of "electronic surveillance" applies to radio communications, but only when the sender and all intended recipients are located in the United States. Subsection (1) of the current definition also applies to radio communications, but only when the surveillance targets a U.S. person in the United States.

[199] The Senate Judiciary Committee's report on FISA explains that "either a wholly domestic telephone call *or an international telephone call* can be the subject of electronic surveillance" – if acquired from a wire in the U.S. or from targeting a U.S. person in the U.S. – but that "most [international] telephonic and telegraphic communications are transmitted at least in part by microwave radio transmissions," leaving them open to surveillance outside FISA if acquired from the radio transmission without targeting a U.S. person in the U.S. FISA Senate Judiciary Report at 33 (emphasis added).

[200] The "directed at" formulation is used elsewhere in FISA, see, *e.g.*, 50 U.S.C. §§ 1802(a)(1)(A), 1804(a)(4)(B), 1805(a)(3)(B), (c)(1)(B), (c)(3) (d). It is also used in Section 2.5 of Executive Order 12333.

[201] Indeed, Subsection (1) of the current definition was added after the other subsections had been established, in what appears to have been (in part, but not in whole) a belt-and-suspenders approach to regulating targeted surveillance of U.S. persons in the United States. See FISA Senate Judiciary Report at 32.

[202] Operation Shamrock was perhaps the government's largest electronic surveillance program (prior to September 11, 2001, in any event), and was conducted by the NSA or its predecessor organizations. For nearly thirty years, from 1945 to 1975, the NSA "received from international cable companies millions of cables which had been sent by American citizens in the reasonable expectation that they would be kept private." Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, Report No. 94-755, Book II at 12 (1976) [hereinafter Church Report]. As the Church Committee Report explains:

> SHAMROCK is the codename for a special program in which NSA received copies of most international telegrams leaving the United States between August 1945 and May 1975. Two of the participating international telegraph companies – RCA Global and ITT World Communications – provided virtually all their international message traffic to NSA. The third, Western Union International, only provided copies of certain foreign traffic from 1945 until 1972. SHAMROCK was probably the largest governmental interception program affecting Americans ever undertaken. Although the total number of telegrams read during its course is not available, NSA estimates that in the last two or three years of SHAMROCK's existence, about 150,660 telegrams per month were reviewed by NSA analysts.
>
> Initially, NSA received copies of international telegrams in the form of microfilm or paper tapes. These were sorted manually to obtain foreign messages. When RCA Global and ITT World Communications switched to magnetic tapes in the 1960s, NSA made copies of these tapes and subjected them to an electronic sorting process. This means that the international telegrams of American citizens on the "watch lists" could be selected out and disseminated.

Church Report Book III at 765 (footnote omitted). I do not mean to sensationalize by this reference to Operation Shamrock; nor is my point dependent on the technical aspects of Shamrock itself. The point is only that, if the government believes that the "particular, known" language in proposed Subsection (1) excludes (some forms of) driftnet surveillance, it could have far-reaching consequences, in part because of changes to the other subsections of the definition that are made by the government's proposal. It would be wise to resolve this issue in an authoritative fashion before changing the law.

[203] Current Subsection (2) does not use this language; it applies only when no party to the communication has consented to the surveillance.

[204] See FISA House Report at 54.

[205] Subsection (2) of the government's proposal refers to a "sender" and "recipients." Although these terms are most comfortably applied to electronic mail messages, FISA has always used them to refer to other forms of communication as well (see, e.g., Subsections (1) and (3) of the current definition), and Subsection (2) of the government's proposal by its terms applies to "any communication."

[206] This assumption is explored at length in the discussion of current FISA, above.

[207] Cf. *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (en banc).

[208] 18 U.S.C. § 2511(1).

[209] 18 U.S.C. § 2511(1)(a) (emphasis added).

[210] 18 U.S.C. § 2511(1)(c) (emphasis added).

[211] 18 U.S.C. § 2511(1)(d) (emphasis added). There are other prohibitions in Title III, see 18 U.S.C. § 2511(1)(b) and (e), but the three provisions quoted in the text are the main ones.

[212] See 18 U.S.C. § 2510.

[213] 50 U.S.C. § 1801(f).

[214] 18 U.S.C. § 2511(2)(e). The terms "officer, employee, or agent" appear to cover everyone within the federal government who might be involved in a FISA surveillance, as well as some non-government personnel, and the requirement that the surveillance be conducted "in the normal course of ... official duty" likely does not significantly restrict the scope of the carve-out. See also 18 U.S.C. § 2511(2)(a)(ii) (authorizing specified third parties to assist the government in carrying out authorized FISA surveillance). These provisions were added to Title III by FISA as "conforming amendments necessary to integrate the Foreign Intelligence Surveillance Act into the existing provisions of [Title III]." FISA House Report at 98. In any event, current FISA itself provides that the FISC may issue an order authorizing surveillance under FISA, and that the Attorney General may authorize surveillance under 50 U.S.C. § 1802, "notwithstanding any other law," which probably is sufficient to insulate FISA surveillance from all other statutory limits. 50 U.S.C. § 1802(a)(1) & (b).

[215] Under 18 U.S.C. § 2511(2)(f), "[n]othing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978."

[216] 50 U.S.C. § 1802(a)(1) (electronic surveillance); see 50 U.S.C. § 1822(a)(1) (nearly identical provision for physical searches). The President authorized the Attorney General to exercise authority under these provisions in Section 1-101 of Executive Order 12139 (for electronic surveillance), and Section 1 of Executive Order 12949 (for physical searches).

[217] 50 U.S.C. §§ 1802(a)(3) (electronic surveillance) & 1822(a)(3) (physical search). FISA also provides that such certifications for electronic surveillance shall be retained by the FISC for "at least ten years." 50 U.S.C. § 1805(h). There is no corresponding provision for physical searches. Cf. 50 U.S.C. § 1824(f). The certification remains under seal unless the government applies for a court order on the ground that, despite expectations, the surveillance or search acquires the communication of, or involves the property of, a U.S. person. See 50 U.S.C. § 1802(a)(3) (electronic surveillance); 50 U.S.C. § 1822(a)(3) (physical search).

[218] 50 U.S.C. § 1802(a)(4) (electronic surveillance); 50 U.S.C. § 1822(a)(4) (physical search). Section 1802 does not expressly authorize physical entry into a foreign power's premises to conduct electronic surveillance, but in 1981 the

Department of Justice reversed its earlier interpretation of the statute and concluded that physical entry was implicitly authorized. See S. Rep. No. 98-660, at 6 (1984) [hereinafter Senate FISA Five Year Report].

[219] FISA House Report at 68.

[220] *Id.*

[221] *Id.*

[222] 50 U.S.C. § 1802(a)(1)(A)(1).

[223] 50 U.S.C. § 1802(a)(1)(A)(2).

[224] 50 U.S.C. § 1822(a)(1)(A)(i).

[225] 50 U.S.C. § 1802(a)(1)(A) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A)(i) (physical search).

[226] See FISA House Report at 29.

[227] *Id.*

[228] Section 1802 refers to "a foreign power" in the singular, while Section 1822 refers to "a foreign power or powers." Nonetheless, Section 1802 is best read to permit surveillance against property controlled exclusively by multiple foreign powers.

[229] Section 1822 authorizes the Attorney General to compel assistance from a "landlord" as well as other persons, strongly suggesting that rental property can fit within its scope. 50 U.S.C. § 1822(a)(4)(A). Thus, despite a landlord's ownership interest, leased property presumably could either be "used exclusively" by or be "under the open and exclusive control" of a foreign power tenant.

[230] FISA House Report at 70. The discussion in the legislative history actually concerns 50 U.S.C. § 1802(b), which is the provision governing ordinary FISA applications. But the phrase "notwithstanding any other law" also appears in 50 U.S.C. § 1802(a).

[231] Vienna Convention on Diplomatic Relations, Article 22, 23 U.S.T. 3227 (Apr. 18, 1961). See also id. at Article 24 ("The archives and documents of the mission shall be inviolable at any time and wherever they may be."); id. at Article 27 ("The official correspondence of the mission shall be inviolable. Official correspondence means all correspondence relating to the mission and its functions ... The diplomatic bag shall not be opened or detained.").

[232] The 1978 legislative history also explains that the phrase "notwithstanding any other law" is meant to overcome any claim that, under 28 U.S.C. § 1251, the FISC cannot approve "surveillance directed at a foreign ambassador." FISA House Report at 70. Section 1802 does not apply where the surveillance is directed at "an agent of a foreign power, rather than at the foreign power itself." H.R. Conf. Rep. No. 95-1720 at 25 (1978).

[233] See Domestic Security Enhancement Act of 2003, Section-by-Section Analysis (Jan. 9, 2003) (available at www.pbs.org/now/politics/patriot2-hi.pdf).

[234] FISA House Report at 69.

[235] 50 U.S.C. § 1802(a)(1)(B) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A)(ii) (physical search).

[236] 50 U.S.C. § 1802(a)(1), (a)(1)(B) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A), (a)(1)(A)(ii) (physical search).

[237] 50 U.S.C. § 1801(a)(2); see FISA House Report at 29.

[238] 50 U.S.C. § 1801(a)(2); see FISA House Report at 29 ("The word 'substantially' means a significant proportion, but it may be less than a majority.").

[239] 50 U.S.C. §§ 1802(a)(1)(C) & (a)(2) (electronic surveillance); 50 U.S.C. § 1822(a)(1)(A)(iii) & (a)(1)(B) & (a)(2) (physical search). The Attorney General must also assess compliance with the minimization procedures and report to the Intelligence Committees as part of his semi-annual reporting obligations. 50 U.S.C. § 1802(a)(2) (electronic surveillance); 50 U.S.C. § 1822(a)(2) (physical search). (There is a mistaken cross-reference in the physical search provisions of FISA. Section 1822(a)(1)(A)(iii) refers to minimization procedures "under paragraphs (1) through (4) of Section 1821(4) of this title," when minimization procedures are in fact set out in paragraphs (A) through (D) of Section 1821(4).)

[240] 50 U.S.C. § 1802(a)(2) (electronic surveillance); 50 U.S.C. § 1822(a)(2)(physical search). See 50 U.S.C. § 1808(a) (semi-annual report on electronic surveillance); 50 U.S.C. § 1826 (same for physical searches).

[241] 50 U.S.C. § 1801(h)(4) (electronic surveillance); 50 U.S.C. § 1821(4)(D) (physical search). This requirement is contained in the statutory definition of "minimization procedures."

[242] In 2003, the Department of Justice wrote in a draft summary of proposed legislation that "[i]n essence, § 1802 authorizes the surveillance of communications between foreign governments, and between a foreign government and its embassy." See Domestic Security Enhancement Act of 2003, Section-by-Section Analysis (Jan. 9, 2003) (available at www.pbs.org/now/politics/patriot2-hi.pdf).

[243] I suspect the government did not intend this, but it is at least a plausible reading, and perhaps the best reading, of the introductory clause of proposed Section 1802A(a) and proposed Section 1802A(a)(3).

[244] See *United States v. Bin Laden*, 126 F. Supp. 2d 264 (SDNY 2000); see also *United States v. Marzook*, 435 F.Supp. 2d 778 (N.D. Ill. 2006).

[245] The Department of Justice has revealed that some FISA applications are "made solely for electronic surveillance, [some] applications [are] made solely for physical search, and [some are] combined applications requesting authority for electronic surveillance and physical search simultaneously." Letter from William E. Moschella, Assistant Attorney General, Office of Legislative Affairs, to L. Ralph Meacham, Director, Administrative Office of the United States Courts (Apr. 30, 2004) (available at www.fas.org/irp/agency/doj/fisa/2003rept.pdf).

[246] 50 U.S.C. §§ 1801(g), 1804, 1823. DOJ has not publicly disclosed whether the Assistant Attorney General has been designated to approve FISA applications.

[247] OIPR is part of the DOJ National Security Division. See 72 Fed. Reg. 10064-01 (Mar. 7, 2007).

[248] FISA's legislative history explains that an application may be filed by "an attorney in the Department of Justice who ha[s] not personally gathered the information contained in the application," and that in such a case "it would be necessary that the application also contain an affidavit by an officer personally attesting to the status and reliability of any informants or other covert sources of information." FISA House Report at 73; *see* S. Rep. No. 103-296, at 60 (1994) [hereinafter FISA Search Senate Report]. The Department of Justice has confirmed publicly that attorneys in OIPR "prepare[] and file[] all applications for electronic surveillance and physical search under the Foreign Intelligence Surveillance Act of 1978," *see* U.S. Dep't of Justice, *Webpage of the Office of Intelligence Policy and Review*, *at* www.usdoj.gov/oipr, and that "OIPR does not conduct investigations," *see* U.S. Dep't of Justice, *Webpage of the Office of Intelligence Policy and Review*, *at* www.usdoj.gov/oipr/fisars.htm. Thus, some other entity, such as the FBI, must investigate, develop, and swear to the facts necessary to support a FISA application. In a speech given at the University of Texas on April 13, 2002, the then-Presiding Judge of the FISC, Royce Lamberth, explained that after reviewing the government's written submissions, "we then have the investigative agent appear before us, under oath, for questioning .... I do ask questions. I get into the nitty-gritty. I know exactly what is going to be done and why. And my questions are answered, in every case, before I approve an application. I know the

same is true of each of my colleagues." Judge Royce Lamberth, The Role of the Judiciary in the War on Terrorism (Apr. 13, 2002) (available at www.pbs.org/wgbh/pages/frontline/shows/sleeper/tools/lamberth.html).

[249] 50 U.S.C. § 1804(a)(1) (electronic surveillance); 50 U.S.C. § 1823(a)(1) (physical search). FISA's legislative history states that the applicant should be "the person who actually presents the application to the judge." FISA House Report at 73. That person is an OIPR (NSD) attorney. To approve the application, a judge of the FISC must find that "the application has been made by a Federal officer." 50 U.S.C. § 1805(a)(2) (electronic surveillance); 50 U.S.C. § 1824(a)(2) (physical search).

[250] In 2006, the word "specific" was added to 50 U.S.C. § 1804(a)(3), which governs electronic surveillance, out of concerns about roving surveillance. See USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006). The word does not appear in the corresponding provision for physical searches, 50 U.S.C. § 1823(a)(3). Orders approving FISA electronic surveillance and physical search applications must specify "the identity, if known, or a description of the [specific] target" of the search or surveillance, again with the word "specific" appearing only in the provision for electronic surveillance orders, 50 U.S.C. § 1805(c)(1)(A), not in the provision for physical search orders, 50 U.S.C. § 1824(c)(1)(A). The provision for electronic surveillance orders makes clear that the FISC's order must specify the identity or a description of the specific target "identified or described in the application." 50 U.S.C. § 1805(c)(1)(A).

[251] As noted earlier, the electronic surveillance provisions of FISA, enacted in 1978, refer to "his belief." 50 U.S.C. § 1804(a)(4). The physical search provisions, enacted in 1994, are gender neutral and refer to "the applicant's belief." 50 U.S.C. § 1823(a)(4).

[252] 50 U.S.C. § 1804(a)(4)(A) (electronic surveillance); 50 U.S.C. § 1823(a)(4)(A) (physical search). Correspondingly, to approve the FISA application, the FISC must find probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3)(A) (electronic surveillance); 50 U.S.C. § 1824(a)(3)(A) (physical search).

[253] 50 U.S.C. § 1804(a)(4)(B). Correspondingly, to approve the FISA electronic surveillance application, the FISC must find probable cause that "each of the facilities or places" to be surveilled "is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). The FISC's order must also specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known." 50 U.S.C. § 1805(c)(1)(B).

[254] Although the application must state that the premises to be physically searched "contains" foreign intelligence information, 50 U.S.C. § 1823(a)(4)(B), there is no requirement of a corresponding specification in a FISC order authorizing a physical search. Nonetheless, this requirement in the application makes the physical search nexus requirements of FISA more like their traditional criminal counterparts.

[255] 50 U.S.C. § 1823(a)(4)(C). Correspondingly, to approve the FISA application, a FISC judge must find probable cause that the premises or property to be searched is "owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power." 50 U.S.C. § 1824(a)(3)(B). Although this provision differs from its counterpart for electronic surveillance in referring to property "used" rather than "used or about to be used" by a foreign power or an agent of a foreign power, *cf.* 50 U.S.C. § 1804(a)(4)(B), the other language in the provision probably makes up for any shortfall. Orders approving FISA physical search applications must also specify "the nature and location of each of the premises or property to be searched." 50 U.S.C. § 1824(c)(1)(B).

[256] 50 U.S.C. § 1804(a)(6). Correspondingly, orders approving FISA applications for electronic surveillance must specify "the type of communications or activities to be subjected to the surveillance." 50 U.S.C. § 1805(c)(1)(C).

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. § 1801(a)(1)-(3) – a foreign government or component, a faction of foreign nations not substantially comprised of U.S. persons, or an entity openly acknowledged to be directed and controlled by a foreign government – and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the

application and order need not specify the type of communications or activities to be subjected to the surveillance. 50 U.S.C. §§ 1804(b), 1805(d). There is no corresponding provision for omitting this description or specification in physical search cases. Section 404 of the government's proposal would eliminate this distinction for official foreign powers.

[257] 50 U.S.C. § 1823(a)(3). This requirement of FISA physical search applications has no corresponding element in the required specifications of a FISC order authorizing a physical search, but orders approving FISA physical search applications must also specify the "type of information, material, or property to be seized, altered, or reproduced." 50 U.S.C. § 1824(c)(1)(C). According to the legislative history, the additional requirement for a "detailed description" in search applications is imposed so that the FISC may "meaningfully assess the sufficiency and appropriateness of the minimization procedures." FISA Search Senate Report at 62.

[258] 50 U.S.C. § 1804(a)(6) (electronic surveillance); 50 U.S.C. § 1823(a)(6) (physical search). Correspondingly, orders approving FISA applications must specify "the type of information" being sought. 50 U.S.C. § 1805(c)(1)(C) (electronic surveillance); 50 U.S.C. § 1824(c)(1)(C) (physical search). The certification that is part of every FISA application for electronic surveillance or a physical search also addresses this.

The precise statutory language governing electronic surveillance applications is "a detailed description of the nature of the information sought," 50 U.S.C. § 1804(a)(6); the precise language governing physical search applications is "a statement of the nature of the foreign intelligence sought," 50 U.S.C. § 1823(a)(6). The legislative history suggests that the two standards are not vastly different. The House Intelligence Committee report on the 1978 statute explains that "[t]he description should be as detailed as possible and sufficiently detailed so as to state clearly what sorts of information the Government seeks. A simple designation of which subdefinition of 'foreign intelligence information' is involved will not suffice." FISA House Report. The Senate Intelligence Committee report on FISA's 1994 physical search provisions states that the "statement should be sufficiently detailed so as to state clearly what foreign intelligence the Government seeks. A simple assertion that 'foreign intelligence information' is sought will not suffice. There must be an explanation of what specific foreign intelligence is sought." FISA Search Senate Report at 62.

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not include this information, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[259] 50 U.S.C. § 1804(a)(5) (electronic surveillance); 50 U.S.C. § 1823(a)(5) (physical search). Correspondingly, to approve a FISA application, the FISC must find that the minimization procedures proposed in the application meet the statutory definition of such procedures, which is set out at 50 U.S.C. §§ 1801(h) and 1821(4). 50 U.S.C. § 1805(a)(4) (electronic surveillance); 50 U.S.C. § 1824(a)(4) (physical search). Orders approving FISA applications must direct that the minimization procedures be followed. 50 U.S.C. § 1805(c)(2)(A) (electronic surveillance); 50 U.S.C. § 1824(c)(2)(A) (physical search).

[260] 50 U.S.C. § 1804(a)(8). Correspondingly, orders approving FISA applications for electronic surveillance must specify "the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance." 50 U.S.C. § 1805(c)(1)(D). Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. § 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the application need not include this information, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[261] 50 U.S.C. § 1823(a)(6). Correspondingly, orders approving FISA applications for physical searches must specify "the manner in which the physical search is to be conducted." 50 U.S.C. § 1824(c)(1)(D). Moreover, although there is no corresponding requirement for physical search applications, "whenever more than one physical search is authorized," the FISC's order must specify "the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search." *Id.* The use of the words "a statement" in this provision is odd; typically, that phrase is used in FISA to describe the contents of an application, not the specifications of an

order. It may be that the asymmetry between physical search applications and orders was unintentional and that Section 1824(c)(1)(D) was originally drafted for inclusion in Section 1823.

[262] 50 U.S.C. § 1824(c)(2)(E); see Foreign Intelligence Surveillance Court Rule 16. There is no corresponding provision in electronic surveillance cases, but the FISC enjoys the power in both electronic surveillance and physical search cases to "assess compliance with the minimization procedures by reviewing the circumstances under which" information concerning U.S. persons was obtained pursuant to the surveillance or search. 50 U.S.C. § 1805(e)(3) (electronic surveillance); 50 U.S.C. § 1824(d)(3) (physical search).

[263] 50 U.S.C. § 1804(a)(9) (electronic surveillance); 50 U.S.C. § 1823(a)(9) (physical search). The two provisions are worded identically, except that the search provision refers to "persons, premises, or property," while the surveillance provision refers to "persons, facilities, or places."

[264] 50 U.S.C. § 1804(a)(10). Orders approving FISA applications for electronic surveillance must specify the "period of time during which the electronic surveillance is approved." 50 U.S.C. § 1805(c)(1)(E).

[265] 50 U.S.C. § 1804(a)(11). Correspondingly, when more than one electronic, mechanical, or other surveillance device is to be used, orders approving FISA applications for electronic surveillance must specify "the authorized coverage of the devices involved and what minimization procedures shall apply to information subject to acquisition by each device." 50 U.S.C. § 1805(c)(1)(F). Although FISA applications for physical searches need not contain any analogous statement, physical search orders must include "a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search." 50 U.S.C. § 1824(c)(1)(D).

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, an application for electronic surveillance need not include this information describing the coverage of individual surveillance devices, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[266] Memorandum from FBI Headquarters, Office of the General Counsel, National Security Law Unit, to all FBI Field Offices, at 1-2 (April 5, 2001) [hereinafter "Woods Procedures"] (available at www.fas.org/irp/agency/doj/fisa/woods.pdf).

[267] The FISC's rules now explicitly permit electronic signatures on documents.

[268] Woods Procedures at 2. The demise of the FISA "wall" and old FISC Rule 11 presumably means that declarations no longer need report as much detail about related criminal investigations or prosecutions.

[269] *Id.*

[270] *Id.* at 2-11.

[271] The Woods Procedures were a response to a series of inaccuracies discovered in two unrelated sets of FISA applications submitted to the FISC in 2000 and 2001. For a more complete discussion of these inaccuracies and the government's response to them, see *In re all Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 611 (FISC 2002), rev'd, *In re Sealed Case*, 310 F.3d 717 (FISCR 2002), and Testimony of David S. Kris before the Senate Judiciary Committee (Sept. 10, 2002) (available at www.usdoj.gov/dag/testimony/2002/krissenjud091002.htm).

[272] 50 U.S.C. § 1804(a)(7) (electronic surveillance); 50 U.S.C. § 1823(a)(7) (physical search). To approve the FISA application, a FISC judge must find that the application "contains all statements and certifications required" by the statute, and "if the target is a United States person, the certification or certifications are not clearly erroneous." 50 U.S.C. § 1805(a)(5) (electronic surveillance); 50 U.S.C. § 1824(a)(5) (physical search).

[273] 50 U.S.C. § 1804(a)(7) (electronic surveillance); 50 U.S.C. § 1823(a)(7) (physical search); *see* 50 U.S.C. § 402; Executive Order 12333 § 1.3(b).

[274] 50 U.S.C. § 1804(a)(7) (electronic surveillance); 50 U.S.C. § 1823(a)(7) (physical search). The two certification provisions are identical except that the physical search provision contains a comma after "President" and provides that the certifying official must be appointed "by and with" rather than merely "with" the advice and consent of the Senate. Any reason for this different phrasing is lost in the historical mist. The certifying officials are designated in Executive Orders 12139 (for electronic surveillance), and 12949 (for physical searches). Both orders were amended in July 2005 by Executive Order 13383, in light of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004). The designated officials (in both amended orders) are: (a) Secretary of State; (b) Secretary of Defense; (c) Director of National Intelligence; (d) Director of the Federal Bureau of Investigation; (e) Deputy Secretary of State; (f) Deputy Secretary of Defense; (g) Director of the Central Intelligence Agency; and (h) Principal Deputy Director for National Intelligence. Under both executive orders, "[n]one of the above officials, nor anyone officially acting in that capacity, may exercise the authority to make the above certifications, unless that official has been appointed by the President with the advice and consent of the Senate."

[275] *See In re* Sealed Case, 310 F.3d 717, 736 (FISCR 2002).

[276] *See* National Security Agency, *Presentation to the House Permanent Select Committee on Intelligence* (2000) (available at www.nsa.gov/releases/HPSCI_04122000/index.htm).

[277] 50 U.S.C. § 1804(a)(7)(A) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(A) (physical search). "Foreign intelligence information" is defined at 50 U.S.C. § 1801(e) (and this definition is incorporated in FISA's physical search provisions, 50 U.S.C. § 1821(1)).

[278] 50 U.S.C. § 1804(a)(7)(B) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(B) (physical search). Prior to the Patriot Act, this provision required certification that "the purpose" of the search or surveillance was to obtain foreign intelligence information; courts interpreted that provision to require that the "primary purpose" be to obtain foreign intelligence information.

[279] 50 U.S.C. § 1804(a)(7)(C) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(C) (physical search).

[280] 50 U.S.C. § 1804(a)(7)(D) (electronic surveillance); 50 U.S.C. § 1823(a)(7)(D) (physical search).

[281] 50 U.S.C. §§ 1804(a)(7)(E)(i)-(ii) (electronic surveillance); 50 U.S.C. §§ 1823(a)(7)(E)(i)-(ii) (physical search). Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, the certification need not include this information. 50 U.S.C. § 1804(b). There is no corresponding provision allowing omission of this element of the certification in physical search cases.

[282] FISA House Report at 76 (referring to the certification as an "affidavit").

[283] *Id.* at 76; *see* FISA Search Senate Report at 62-63. The Foreign Intelligence Surveillance Court of Review has also emphasized the importance of the certification. *See In re* Sealed Case, 310 F.3d 717, 736 (FISCR 2002).

[284] 50 U.S.C. §§ 1804(d), 1805(a)(5) (electronic surveillance); 50 U.S.C. §§ 1823(c), 1824(a)(5) (physical search); FISA House Report at 75.

[285] 50 U.S.C. § 1804(a)(2) (electronic surveillance); 50 U.S.C. § 1823(a)(2) (electronic surveillance). Correspondingly, to approve the FISA application, a FISC judge must find that the President has authorized the Attorney General to make the application. 50 U.S.C. § 1805(a)(1) (electronic surveillance); 50 U.S.C. § 1824(a)(1) (physical search). The President authorized the Attorney General to make FISA electronic surveillance applications in Executive Order No. 12139, and to make FISA physical search applications in Executive Order No. 12949. In addition, Executive Order 12333 provides that the "Attorney General hereby is delegated the power to approve the

use for intelligence purposes, *within the United States* or against a United States person abroad, of any technique for which a warrant would be required if undertaken for law enforcement purposes." Exec. Order No. 12333 § 2.5 (emphasis added). This language was originally included to permit the Attorney General to authorize domestic physical searches in foreign intelligence cases, before FISA was amended (in 1994) to authorize such searches, FISA Search Senate Report at 37, but it would probably also satisfy FISA's requirement for Presidential authorization in electronic surveillance cases.

[286] 50 U.S.C. § 1804(a) (electronic surveillance); 50 U.S.C. § 1823(a) (physical search). Correspondingly, to approve the FISA application, a FISC judge must find that the Attorney General (as defined in the statute) has approved the application for filing. 50 U.S.C. § 1805(a)(2) (electronic surveillance); 50 U.S.C. § 1824(a)(2) (physical search). There is no requirement in FISA that the President approve individual FISA applications, although Presidents have done so in at least some cases. *See* Exec. Order No. 12036 §§ 2-201& 2-204; FISA Search Senate Report at 32-33, 59.

[287] FISA House Report at 73; *see* FISA Search Senate Report at 60-61.

[288] 50 U.S.C. § 1804(c) (electronic surveillance); 50 U.S.C. § 1823(b) (physical search). Correspondingly, the FISC may require a FISA applicant to submit additional information "as may be necessary to make the determinations required" under the statute. 50 U.S.C. § 1804(d) (electronic surveillance); 50 U.S.C. § 1823(c) (physical search). See also Foreign Intelligence Surveillance Court R. 10(d).

[289] 50 U.S.C. §§ 1804(e), 1824(d).

[290] *Id.*

[291] *Id.*

[292] *Id.* These provisions were enacted as part of the Intelligence Authorization Act for Fiscal Year 2001. Pub. L. No. 106-567, § 602(a), 114 Stat. 2831 (Dec. 27, 2000). Senator Specter, a key sponsor of the legislation, explained his view that they were necessary in light of DOJ's handling of the investigation of Wen Ho Lee. Reviewing what he believed were errors in the initial DOJ decision not to seek a FISA authorization in that case, Senator Specter went on to explain what (in his view) happened next:

> When [an] FBI Assistant Director ... raised the FISA problem with the Attorney General on August 20, 1997, she delegated a review of the matter to [an Associate Deputy Attorney General, or ADAG], who had virtually no experience in FISA issues. It is not surprising then, that [the ADAG] again applied the wrong standard for probable cause. He used the criminal standard, which requires that the facility in question be used in the commission of an offense, and with which he was more familiar, rather than the relevant FISA standard which simply requires that the facility "is being used, or is about to be used, by a foreign power or an agent of a foreign power."

146 CONG. REC. S9685-01 (daily ed. Oct. 3, 2000). Senator Specter's account is substantially similar to, and may be drawn from, the account set forth in the *Final Report of the Attorney General's Review Team (AGRT) on the Handling of the Los Alamos National Laboratory Investigation* ("[R]eview of the [FISA] application should not have been assigned to an Associate Deputy Attorney General who, despite his other considerable qualifications and expertise, had almost no prior experience with FISA applications .... The ADAG should have met with the FBI, and not just with OIPR, before determining that OIPR's evaluation of the application was correct .... The ADAG reached the wrong judgment .... The ADAG should have reported his findings to the Attorney General, who was never advised that the ADAG had decided the matter against the FBI.").

[293] The term "United States person" is defined in 50 U.S.C. § 1801(i) (and the definition is incorporated for physical search cases by 50 U.S.C. § 1821(1)).

[294] 50 U.S.C. § 1823(a)(8). The special concern about physical searches of U.S. persons' residences is understandable, but as a technical matter this is a curious provision because it overlaps substantially with the requirement of a certification (from a high-level, Senate-confirmed official) that the information being sought in the search "cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1823(a)(7)(C). The certification must also contain "a statement explaining the basis" for that certification. 50 U.S.C. § 1823(a)(7)(E). The legislative history explains that the provision was added by the conference committee because of the "special concerns and sensitivities" involved in searching U.S. persons' residences and that the provision means to go beyond the certification requirement in the level of detail provided. FISA Search Conference Report at 58-59. By negative implication, however, it tends to suggest that certifications need not be very detailed. The conferees also apparently believed that requiring this statement from the Attorney General – rather than the certifying official – would further emphasize its importance.

[295] 50 U.S.C. § 1801(g). DOJ has not publicly revealed whether the Assistant Attorney General has been designated to approve FISA applications.

[296] 50 U.S.C. § 1804(a)(11).

Where the target of electronic surveillance is a foreign power as defined in 50 U.S.C. §§ 1801(a)(1)-(3), and each of the facilities or places at which the surveillance is directed is owned, leased, or exclusively used by that foreign power, an application for electronic surveillance need not include this information describing the coverage of individual surveillance devices, and the order need not specify it. 50 U.S.C. §§ 1804(b), 1805(d).

[297] 50 U.S.C. § 1804(a)(2).

[298] See 18 U.S.C. § 921(4)(B) (referring to a weapon "which has a barrel with a bore of more than one-half inch in diameter").

Center for National Security Studies

Protecting civil liberties and human rights

Statement of the Center for National Security Studies

by Kate Martin, Director, and Lisa Graves, Deputy Director

"Constitutional Failings of the Foreign Intelligence Surveillance Modernization Act"

Before the Senate Select Committee on Intelligence

May 1, 2007

On behalf of the Center for National Security Studies, we thank Chairman Rockefeller for the invitation to submit our views regarding the Foreign Intelligence Surveillance Act (FISA) and the administration's proposal to amend it via the "Foreign Intelligence Surveillance Modernization Act" (FISMA).

The Center has worked on issues concerning FISA since its birth, and we are pleased to be invited to share our views with the distinguished Members of this Committee who are charged with shared oversight of US intelligence-gathering operations. For more than 30 years, the Center has worked to ensure that civil liberties and human rights are not eroded in the name of national security. We are guided by the conviction that our national security can and must be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and, that by doing so, solutions to apparent conflicts can often be found without compromising either.

Summary. We strongly oppose the administration's proposal and urge the Committee to reject it because its complex changes to FISA would severely undermine the fundamental privacy rights of Americans. It would authorize the Executive Branch to conduct unconstitutional searches of Americans' private conversations. It would permit the government intentionally to acquire billions and billions of Americans' international phone calls and e-mails without a warrant, so long as it vacuumed up the contents of these communications en masse, rather than targeting for initial acquisition the communications of a particular individual in the United States. And it would permit the government to then sort and analyze all those

1120 19th Street, NW, Suite 800, Washington, DC 20036
(202) 721-5650 fax: (202) 530-0128 cnss@cnss.org www.cnss.org

communications and listen to and distribute whichever ones it chose, in secret, with no warrant or meaningful individualized oversight whatsoever. This would be a dramatic and drastic change to statutory law. Under the guise of "tech neutrality," the proposal would neutralize the key protections in current law and authorize warrantless surveillance of virtually all communications in any form by Americans with anyone, including other Americans, located overseas. The administration's proposal attempts to make public law sanction federal government acquisition and mining of vast amounts of private, personal information on Americans residents, preying on fears about terrorism and exploiting new technologies that make such invasions of the private calls and e-mails of American residents easier than ever before.

The administration has tried to cast its proposal as merely "modernization," even though FISA has been repeatedly modernized including four significant changes since September 11th. In each instance, Congress has kept the basic structure of individualized judicial checks for communications to or from people in the US, and rightly so. As General Hayden testified to the House Permanent Select Committee on Intelligence in 2000, the reality is that FISA's "privacy framework is technology neutral and does not require amendment to accommodate new communications technologies." Notably, he gave this assurance after calling reports that the NSA operated a program called "Echelon" to monitor all international communications, "false and misleading," yet the administration's FISMA tries to give legal license to such activities directed at streams of American communications. The changes being proposed would not be mere accommodations of new technologies in order to keep the legal framework current but would work a fundamental change to the structure of law and substantially weaken civil liberties protections. Indeed, the fact that more human thought and speech than ever before is now transcribed into electronic signals and transmitted by phone calls or e-mails requires greater protections for privacy and freedom of speech, not fewer.

The Administration seeks to legalize massive warrantless surveillance of Americans, far beyond the surveillance it has admitted to in the "Terrorist Surveillance Program."

We now know that since shortly after the 9/11 attacks the administration has claimed the power to listen to Americans' conversations and read their e-mails without warrants and in violation of FISA's protections for the privacy of people in the US in both their international and domestic communications. We do not yet know how broadly they exercised that power for the duration of the program, although they have admitted to warrantless surveillance of some

international communications of persons in the US, all the while the President and others in the administration claimed publicly, until late 2005, that they obtained warrants to monitor people here. There is also evidence that they have sought addressing information of all communications presumably in order to conduct traffic analysis of billions of communications by Americans.

The administration argued when the warrantless surveillance was first revealed, that the President has "inherent" powers as commander-in-chief to set aside the requirements of FISA, if he believes it necessary. This argument ignored the first Article of the Constitution, which expressly commits to Congress shared powers over war and national defense and the system of separated but shared powers described by the Supreme Court in the steel seizure case, even in times of war. So, the administration also contended that the Authorization for the Use of Military Force in Afghanistan constituted an implicit amendment to FISA authorizing warrantless surveillance of people in the US. After much scholarly and bipartisan rejection of these arguments, the administration apparently pressed for a creative interpretation of the law by the FISA court to authorize some part of the most current iteration of such surveillance. The purpose of the administration's proposed amendments is illuminated when set in this context. While the administration has not disavowed its claims of executive power to override the law, it is now pressing for statutory changes to achieve the same end, *i.e.*, unchecked secret power to conduct electronic surveillance on millions of Americans.

*** The bill would permit the vacuuming of all international communications of Americans.** The bill would allow the warrantless seizure of all international calls and e-mails of American residents and businesses, without any link to al Qaeda—a sweep far broader than the secret program President Bush publicly acknowledged on December 17, 2005. It would change the definition of "electronic surveillance" to allow Americans' international calls and e-mails to be scooped up en masse through any technological means (*i.e., "tech neutral")* so long as a particular American was not targeted in the *initial* "acquisition" or surveillance.[1] Once

[1] This radical change is buried in the technical amendments to the sophisticated definition of "electronic surveillance" in FISA, which can be unpacked as follows. Current FISA law bars the warrantless "acquisition" of the content of domestic communications--whether they occur by *wire or radio*--as well as "information," if it is intentionally acquired through other means, such as "bugging" or video surveillance devices, where a person has a reasonable expectation of privacy. FISA also bars warrantless "acquisition" in the US of the contents of *wire* communications "to or from a person in the United States," meaning domestic or international, whether a known US person is the target of the acquisition or not. It also bars the surveillance of

Americans' international communications were acquired without a warrant, the government would be free to analyze and listen to any private personal or business conversations or data, without ever having obtained any judicial warrant. The "Fact Sheet" issued by the Department of Justice omits any mention of this and the other extraordinary changes that would be made by the bill. No administration official has explained to the American people that this is the power they are seeking.

*** The bill would also apparently authorize warrantless access to some number of purely domestic cell phone and e-mail content**, with a new statutory basis to claim that the government does not know and need not ascertain if the sender and all recipients are in the US.

*** It would permit unlimited access without court oversight to all international and some domestic call records**, allowing the tracing of the social networks of American residents, including journalists as a routine part of foreign intelligence monitoring here.

*** The changes to FISA's definitions would also create a loophole for surreptitious video surveillance of private spaces without a warrant for foreign intelligence purposes.**

*** The administration's bill also replaces the narrow exception to the warrant requirement for certain communications of embassies in the US with broader authority to acquire communications in the US without a court order**, simply based on the Attorney General's certification or directive. For example, section 102 of FISA would be changed to eliminate the narrow exception that a warrant is not required if the surveillance is directed "solely" at the communications of foreign governments in the US, and it deletes the bar on such warrantless surveillance even when there is a "substantial likelihood" Americans' conversations will be swept in. That is, the Attorney General could order warrantless surveillance directed toward a foreign government here even if such surveillance was likely to sweep in Americans' conversations. And the bill strikes the statutory protections for American conversations obtained

---

the contents of the *radio* communications to or from a known US person in this country by intentionally "targeting" that person. (The statute is silent about acquiring international *radio* communications without intentionally targeting a particular US person, although at the time FISA was passed Congress recognized that Americans do have Fourth Amendment rights in the privacy of the content of such communications.) By repealing or modifying these statutory prohibitions, the bill would suddenly allow the warrantless acquisition of the content of all international telephone, e-mail or other communications sent by any technology to or from Americans so long as it is acquired en masse rather than by *initially* targeting a particular US person's communications.

inadvertently in this way without warrants, by eliminating FISA's requirement in 50 USC 1801(h)(4) that such conversations be deleted within three days of acquisition unless the government obtains a FISA court order or if there is a threat to life or threat of bodily injury.

It is quite likely that any power granted to gather information will be used to the maximum extent, and the powers proposed to itself by the administration would be used to sweep up conversations and communications involving millions of innocent people. As Mark Twain said, "to a man with a hammer, everything looks like a nail." These proposals strike at the heart of Americans' reasonable expectations of privacy against government surveillance.

The Bill would violate the Fourth Amendment.

The warrantless surveillance of Americans' conversations that would be authorized by FISMA fundamentally violates the Constitution because:

- The Fourth Amendment requires warrants, and there is a FISA court available to issue such warrants;
- It requires an individualized determination of probable cause before seizing private communications;
- and the massive surveillance that would be authorized by this bill would be unreasonable, under any fair interpretation of the Fourth Amendment.

In addition, the administration is simply wrong that, contrary to the language and legislative history of FISA, Congress intended to allow virtually unlimited monitoring of the content of Americans' international communications or believed that such acts would be constitutional.

Faithful enforcement of the Fourth Amendment's protections are in some ways even more critical for intelligence surveillance than for criminal investigations because intelligence surveillance is likely to remain secret. On this point, the bipartisan Church Committee recorded what can happen, even with he best of intentions of protecting the country, when warrants are not required. Unchecked secret government power intended to protect the national security:

> may become a menace to free government and free institutions because it carries with it the possibility of abuses of power which are not always quickly apprehended or understood.... Our investigation has confirmed that warning. We have seen segments of our government, in their attitudes and actions, adopt tactics unworthy of a democracy.... *We have seen a consistent pattern in which programs initiated with limited goals*, such as preventing criminal violence or identifying foreign spies, were *expanded to what witnesses characterized as "vacuum cleaners," sweeping in information about lawful activities of American citizens.*

Final Report of the Senate Select Committee, Book II, April 26, 1976 (emphasis added). Notably, the Defense Department has agreed with this assessment:

> In the early and mid 1970s several Congressional committees, including the Church, Pike, and Ervin committees, conducted investigations and public hearings. After three and a half years of investigation, these committees determined that what had occurred was a classic example of what we would today call "mission creep." What had begun as a simple requirement to provide basic intelligence to commanders charged with assisting in the maintenance and restoration of order had become a monumentally intrusive effort. This resulted in the monitoring of activities of innocent persons involved in the constitutionally protected expression of their views on civil rights or anti-war activities. The information collected on the persons targeted by Defense intelligence personnel was entered into a national data bank and made available to civilian law enforcement authorities. This produced a chilling effect on political expression by those who were legally working for political change in domestic and foreign policies. Senator Ervin concluded "the collection and computerization of information by government must be tempered with an appreciation of the basic rights of the individual, of his right to privacy, to express himself freely and associate with whom he chooses." As a result of these investigations, DoD imposed severe restrictions on future surveillance of U.S. persons, required that information already in DoD files be destroyed, and established a structure to regulate future DoD intelligence collection.

Available at: http://www.dod.mil/atsdio/. Unfortunately, over the past six years, we have seen frequent reports of deliberate, secret departures from these and other protections, some of which have been reportedly abandoned only last month, as with the TALON database.

On electronic surveillance, only the most extreme proponents of unchecked presidential power argue that warrantless surveillance conducted in violation of FISA's prohibitions is legal. But eliminating FISA's statutory prohibitions will not cure the constitutional infirmity of such surveillance. The Fourth Amendment is clear that a judicial warrant is required to seize or search an Americans' private papers or the equivalent and plainly such warrants must be based on individualized probable cause of wrongdoing, such as conspiring with foreign nationals to commit acts of terrorism.

The Fourth Amendment protects the privacy of the people of the United States and requires warrants before listening to conversations. *Katz v. United States*, 389 U.S. 347 (1967). Notably, in a case involving warrantless wiretapping in the name of national security, the Supreme Court stressed that "Fourth Amendment freedoms cannot properly be guaranteed if domestic surveillance may be conducted solely within the discretion of the Executive Branch." *United States v. United States District Court*, 407 U.S. 297, 324 (1972). While the Court

reaffirmed that "prior judicial approval is required for the type of domestic surveillance" in that case, it invited Congress to create standards for domestic and foreign intelligence gathering to protect constitutional rights. *Id.* In passing FISA after both a complete committee investigation and extensive public hearings, the Senate noted that the statute "was designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 7, 1978 U.S.C.C.A.N. 3904, 3908. There is no Fourth Amendment exception for the seizure of Americans' international calls, whether made from a landline, cordless phone or cell phone, or written in e-mails, although that is what the bill attempts to create. And there is no emergency exception to the Fourth Amendment that could accommodate what the administration desires.

When the government wants to monitor the communications of a person in the US, then the Constitution as reflected in FISA requires that there be judicial scrutiny. And, Congress has established the FISA court as a workable mechanism for issuing classified judicial warrants. Nevertheless, in a departure from these norms, the Department of Justice has cited three cases allowing warrantless surveillance while neglecting the fact that each of these cases dealt with pre-FISA surveillance before Congress either made detailed findings that the unchecked regime of warrantless surveillance was a violation of the Fourth Amendment or created the FISA court. *See United States v. Truong*, 629 F.2d 908, 916 (4th Cir. 1980); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc); *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973). The administration also often ignores contrary precedent such as *Zweibon v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc), where a plurality of the D.C. Circuit rejected the notion that electronic surveillance for foreign intelligence activities can be conducted without a warrant. (Nor is the dicta about supposed inherent authority in the 2002 FISCR decision binding or persuasive authority in the face of Congress' explicit enactments.) Congress passed FISA because of the absolute imperative to "provide the secure framework by which the executive branch may conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this nation's commitment to privacy and individual rights." S. Rep. No. 95-604, pt. 1, at 15 (1977) (noting that courts had "held that a warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of, nor acting in collaboration with, a foreign power").

Even if FISA's warrant requirements were recklessly repealed and warrantless electronic surveillance of Americans were not confined by statute, the Fourth Amendment would still require that the Attorney General (or a comparable high-level official) personally determine there is probable cause that the target of the surveillance is an agent of a foreign power who is engaged in espionage or terrorism-related activities. *See United States v. Truong*, 629 F.2d 908, 916 (4th Cir. 1980). In that case, the Attorney General made no such determination, the search was held unconstitutional and the court suppressed evidence from the search.

The administration's proposal would authorize massive surveillance of Americans with no warrant and not even any individualized determination of probable cause by the Attorney General. Perhaps the administration will argue that because the bill would only allow the "untargeted" surveillance of thousands or millions of Americans, the requirement of individualized probable cause is inapplicable, although privacy would still be warrantlessly invaded. And, by any reasonable estimate of the number of actual suspected al Qaeda operatives in contact with the US, the volume of innocent communications of Americans that would be swept up in a nation of 300,000,000 people creates a ratio exponentially smaller than even the so-called one percent doctrine of the Vice President. Statistically, the proportion of innocent international calls and e-mails that would be statutorily allowed to be vacuumed under this proposal would be on the order of 99.999+ innocent--and, at what cost in both privacy and money? There is no such exception in the Fourth Amendment. The Constitution does not permit the seizure of millions or billions of conversations or e-mails of Americans to look for a few.

The administration's proposal would repeal a major protection in FISA.

Since the enactment of FISA, no administration has ever explained to the American people that despite the law, there is no privacy in their international communications against seizure or search by the federal government, should they happen to be carried wirelessly. Nor has this administration explained that such is its view. Nevertheless, the administration now argues for a proposal to effectuate such a result, on the ground that it is simply "updating" FISA in light of technological developments.

But allowing such warrantless vacuum cleaner surveillance would be a major repeal of FISA's protections. The plain language of FISA bars the acquisition of the contents of calls "to or from Americans" without a FISA warrant through tapping wire communications in the US. This command plainly was intended to protect against the wiretapping of Americans'

international and domestic calls and telegrams. As the Church Committee noted, the fact that the NSA's "Operation Shamrock" gathered all international telegrams of Americans without initial targeting was of little consolation to those Americans whose private correspondence was seized and analyzed. FISA forbids the government from warrantlessly tapping wires in the US, whether they are telephone lines strung from city to city or trans-oceanic cables departing the coasts. These protections defined in 50 USC 1801(f)(2), bar warrantless acquisition whether a particular person is targeted or whether no one or everyone is targeted. It bars "sitting on the wire." This section would be deleted in its entirety by the administration's bill.

In place of (f)(2), the administration proposes to make 1801(f)(1) "technologically neutral," but does so in a way that eliminates the bar on blanket acquisition of international calls to or from Americans via warrantless wiretapping. Under the administration's revision, there would be no bar on acquisition of all international communications, by sitting on a wire/cable in the US and seizing all such communications of Americans.

The administration's claim that Congress intended to allow it virtually unfettered access to all Americans' international communications unless a person were targeted initially is contradicted by the legislative history. While the so-called "radio exception" in (f)(1) excludes non-targeted international radio transmissions from FISA, Congress made clear that exclusion of some surveillance of Americans from FISA's definitions "should not be viewed as congressional authorization of such activities as they affect the privacy interests of Americans," noting that in any case, "the requirements of the Fourth Amendment would, of course, continue to apply to this type of communications intelligence activity," regardless of FISA. *See* H. REP. NO. 95-1283(I) (June 5, 1978).

Moreover, Congress made clear that when it barred the intentional "targeting" of radio transmissions of Americans, beyond barring the warrantless wiretapping of calls to or from people in the US, that it would not brook the very scenario implied by the administration's interpretations this past year: initial, untargeted acquisition, followed by targeted searches of Americans' acquired conversations. Specifically, the administration suggested in the course of its work on the Wilson and Specter bills that it did not believe FISA placed any limits on the use of devices that analyze communications "lawfully" acquired, such as through its warrantless surveillance of Americans that it has argued is lawful. While FISA did not settle rules for the monitoring of foreign nationals outside the US, it was focused on securing the rights of people in

the US against invasions of privacy, including drilling down in radio signals to monitor frequencies containing channels of American transmissions, and this is reflected in both the legislative history and in long-standing internal directives to NSA operators in the field against intentionally monitoring Americans, even if not known by name, at least before this administration took over.

Telecommunications history also does not support the administration's claims.

The administration's fall back argument is the assertion that in 1978 most international communication was via radio and most domestic communication was via wire but now the situation is reversed—meaning they claim that technological changes are denying them easy access to most international communications of Americans that they claim to be *entitled* to. Beyond the legal history and language in FISA against that interpretation, even a general examination of telecommunications history reveals that the scenario they posit claiming that virtually all international calls of Americans were via satellite radio and therefore intended to be obtained by the government is not accurate. While satellites were increasingly used in the 1970s for television broadcasting and some telecommunications, American telephone companies were continuing to rely on trans-oceanic cables for international calls, with newer transatlantic cables sunk even the year after FISA passed, followed by newer Pacific cables in the early 1980s, which were then replaced in the late 1980s by fiber optic cables that made calls easier to hear and faster. These historic facts are undeniable and anyone old enough to have made international calls in the late 1970s and early 80s undoubtedly remembers the effect of those wire cables: international phone calls sounded a bit like a tunnel and there was a slight delay in response. That is not to say that US calls were transmitted exclusively by wire; in fact, regional domestic calls at the time FISA was passed were often transmitted in part by microwave radio towers, and now they may be transmitted wirelessly by cellular towers and by domestic fiber optic cable.

A more accurate statement than the administration's description would be that for past 29 years, US telecommunications has relied on both wire and radio technology for domestic and international calls. From the beginning, FISA was written to accommodate that reality. There are some conceptual differences between radio and wire communications, for example with the use of satellites for television and radio broadcasts to the public or the necessity of SIGINT regarding the radio communications of navy ships or submarines. But the American people did not, and do not, believe the government has a right or was given statutory authority to monitor all

international communications of Americans in the aftermath of documented abuses by the NSA and other intelligence agencies through secret programs, such as Operation Shamrock and Operation Minaret. There is no evidence that Congress intended, or that the NSA has for the past 30 years, indiscriminately seized millions of conversations and communications of people in the US for analysis. On the contrary, the NSA's own guidance in USSID 18, even provided protections for the content of the communications of Americans abroad.

FISA also bars the government from intentionally acquiring the purely domestic radio communications of Americans when there is a reasonable expectation of privacy because Americans do not lose their constitutional right to privacy merely because telephone companies beam their domestic calls beam them to or from microwave towers. But current law does not bar the government from hearing short-wave radio broadcasts or from listening to embassy communications that are unlikely to include Americans communications or monitoring foreign-to-foreign communications beyond the reach of the Fourth Amendment. But improvements in electronic communications, such as the use of fiber optic cables or the advent of the Internet, simply do not justify fewer protections for privacy as this bill proposes.

The massive surveillance that would be permissible under the bill is not reasonable under the Fourth Amendment, let alone consistent with the warrant requirement.

Even the administration concedes that seizure of the contents of Americans' private communications must be reasonable, while claiming that their actions are reasonable. But the massive surveillance that would be allowed by this bill is manifestly unreasonable. The core of the Fourth Amendment is protection against unreasonable "general searches," especially of individual's private thoughts and communications. The administration, in essence, claims that Americans have no reasonable expectations of privacy in any of their international communications by phone or e-mail, as long as the government does not target them individually. Instead of offering facts and evidence that allowing the unchecked acquisition of virtually all international communications by Americans is the only way to protect against acts of terror in the US, the administration retreats to its standard mantra of national security justifications that, as former National Security Advisor Zbigniew Brzezinski pointed out, is counter-productive fear-mongering. Zbigniew Brzezinski, "Terrorized by 'War on Terror,'" *The Washington Post*, March 25, 2007.

The American people are entitled to know the basis for the claim that such massive invasions of Americans' private calls and e-mails is likely to be effective, much less necessary and proportionate. Generalizations based on a few extrapolations are not enough, claims of past successes must be examined as to whether the same result could have been achieved differently with less cost to civil liberties. There needs to be a thorough examination and analysis of the following: What is the range of the likely threat from individuals in this country, including Americans? How many international communications would be subject to surveillance, presumably millions every day for years to come? What is the likely number of communications that would yield useful intelligence, presumably a very small fraction of the communications actually seized? What are the costs of such a program, in terms of dollars and resources, such as translators allocated to this and therefore unavailable for other more focused, counterterrorism measures? What is the present and future risk to individual liberties from giving the government unchecked power to seize and listen to the private communications of millions of Americans? What is the cost in terms of loss of public trust in democratic and accountable government? What are the opportunity costs in terms of other security measures that could be funded to greater effect or without eroding core privacy rights of a free people?

These are difficult questions and some of the details underlying the answers are properly secret. But this administration has demonstrated time and again that its public statements on this and other intelligence issues are not credible and that it keeps facts secret that contradict its public assurances. The Congress cannot, consistent with its constitutional responsibility, legislate on this proposal without a much fuller public record and debate. Such a searching probe is essential to the preservation of the Constitution, no matter who is in the White House because, as the framers understood and provided against, over-reaching represents the fundamental tendency of individuals and factions in power, especially in times of national threat.

On Warrantless Access to Foreign-to-Foreign Communications.

The DOJ's Fact Sheet on the bill claims that it "would . . . protect civil liberties and privacy interests and improve our intelligence capabilities by focusing FISA on people located in the US. Revolutions in telecommunications technology have brought within FISA's scope communications that Congress did not intend to be covered—and, as a result, extensive resources are now expended obtaining court approval for acquiring communications that do not directly or substantially involve the privacy interests of Americans." But, as outlined above, the

administration would expressly delete long-standing privacy protections for the millions of people in the US by *exempting* the acquisition and later analysis of all international conversations from FISA. We would agree, however, that in crafting FISA Congress did not intend to place rules on the monitoring of what has been called "foreign-to-foreign" communications. That is why we support the tailored fix in Senator Feinstein's, S. 1114, which would deal with the new situation, in which the communications of two people outside the US who are not US persons are routed through US switches, by making clear no warrant is needed for that. The administration's proposed language goes way beyond that fix.

Similarly, if the government does not have enough resources to process FISA warrants for searching Americans' conversations or homes in order to protect both security and privacy, it should endorse Senator Feinstein and Congresswoman Harman's proposals to provide more resources for the FISA process.

All three branches must act to safeguard civil liberties consistent with the needs of national security and there must be a public debate.

Having seen that executive branch rules and congressional oversight were insufficient to protect civil liberties and national security without statutory rules, Congress enacted FISA. It also reiterated that public debate is necessary for a proper resolution of the terms of such laws.

> This evidence alone should demonstrate the inappropriateness of relying solely on executive branch discretion to safeguard civil liberties . . . . Even the creation of intelligence oversight committee should not be considered a sufficient safeguard, for in overseeing classified procedures the committees respect their classification, and the result is that the standards for and limitations on foreign intelligence surveillances may be hidden from public view. In such a situation, the rest of the Congress and the American people need to be assured that the oversight is having its intended consequences–the safeguarding of civil liberties consistent with the needs of national security. **While oversight can be, and the committee intends it to be, an important adjunct to control of intelligence activities, it cannot substitute for public laws, publicly debated and adopted, which specify under what circumstances and under what restrictions electronic surveillance for foreign intelligence purposes can be conducted.** Finally, the decision as to the standards governing when and how foreign intelligence electronic surveillance should be conducted is and should be a political decision, in the best sense of the term, because it involves the weighing of important public policy concerns–civil liberties and national security . . . . Under our Constitution legislation is the embodiment of just such political decisions.

H. REP. NO. 95-1283, at 21-22 (emphasis added). We firmly believe that the administration's proposal would circumvent the purpose of FISA through clever re-definition of what is governed

by FISA's warrant requirements, even though the statute "was designed . . . to curb the practice by which the Executive Branch may conduct warrantless electronic surveillance on its own unilateral determination that national security justifies it." S. Rep. No. 95-604(I), at 7, 1978 USCCAN 3904, 3908. The administration's proposal would resurrect that practice and seeks to do so without any informed public debate about its intention. We commend the Committee for its oversight and inquiry thus far. Changes this far-reaching *require* extensive public debate.

Conclusion. In FISA, Congress recognized since the beginning of the digital revolutions that emerging technology requires more protections for privacy rather than fewer, as more and more human thought and speech is committed to electronic documentation. As Senator Sam Ervin, the chief architect of the Privacy Act, which was intended to prevent computerized government dossiers, put it:

> [D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom . . . . Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.

Senator Ervin, on June 11, 1974, *reprinted in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, S.3418, at 157 (Public Law 93-579)(Sept. 1976).

The Center for National Security Studies appreciates the Committee and its staff for considering these vitally important issues. We have set forth our request for additional public hearings on these matters, in a joint letter with other organizations submitted to the Chairman. We have also transmitted for the record a rebuttal of additional arguments made by the administration in its press relations regarding this proposed legislation (such as relating to data-mining, immunity, and other serious concerns we have regarding the bill). We hope this is the beginning of many public hearings on these matters, and we thank you for considering our views on this proposal.

Facts v. Fiction: The Justice Department's "New" Re-Write of FISA

Prepared by Lisa Graves, Deputy Director, Center for National Security Studies (4-18-07)
For further information, contact Lisa Graves or Kate Martin, Director of CNSS, at 721-5650

The Justice Department's "Fact Sheet" about its 2007 FISA bill omits the most important effect of its proposed changes: it would permit the government to acquire millions of Americans' international phone calls and e-mails without a warrant, so long as it vacuumed up the contents of these communications en masse, rather than targeting for acquisition the calls of a particular individual in the United States. And it would permit the government to then sort and analyze all those communications and listen to and distribute whichever ones it chose, in secret, with no warrant or meaningful oversight whatsoever. This would be a dramatic and drastic change to current law. Under the guise of "tech neutrality," the proposal would neutralize important protections in current law and authorize the warrantless surveillance of virtually all communications by Americans with anyone, including other Americans, located overseas.*

The bill would permit the vacuuming of all international communications of Americans. The bill would allow wholesale vacuuming of the international communications of American individuals and businesses by the NSA without judicial approval under FISA. For the content of domestic communications, these would require a warrant under FISA, if the government has "reason to believe" the sender and all recipients are actually located in the US. It is noteworthy that administration officials have said in recent testimony that "there are no zip codes on the world wide web" and that a cell phone number does not necessarily indicate where a particular phone call is made—so the administration may intend this new language to support a statutory presumption that the senders and receivers of some number of domestic e-mails and cell calls are not located in the US and are thus not subject to the warrant requirement. It also appears that the changes to FISA's definitions could create a loophole for surreptitious video surveillance of private spaces without a warrant being required by the foreign intelligence statute. It is also noteworthy that the administration signaled last year that it believes that "surveillance" does not include devices used for analyzing, selecting out, or mining content or data lawfully acquired, and the bill would vastly expand what can be "lawfully" acquired without warrants under FISA.

The bill's changes are not modest updates to modernize FISA and increase privacy, but would dramatically change the law and substantially weaken civil liberties protections in current law. In 2000, General Hayden testified that FISA's "privacy framework is technology neutral and does not require amendment to accommodate new communications technologies." The recent administration claims regarding this proposal stand in stark contrast to that accurate admission.

Accordingly, the Center for National Security Studies strongly opposes this proposed legislation.

---

* This radical change is buried in the technical amendments to the sophisticated definition of "electronic surveillance" in FISA, which can be unpacked as follows. Current FISA law bars the warrantless "acquisition" of the content of domestic communications–whether they occur by *wire or radio*–as well as "information," if it is intentionally acquired through other means, such as "bugging" or video devices, where a person has a reasonable expectation of privacy. FISA also bars warrantless "acquisition" in the US of the contents of *wire* communications "to or from a person in the United States," meaning domestic or international, whether a known US person is the target of the acquisition or not. It also bars the surveillance of the contents of the *radio* communications to or from a known US person in this country by intentionally "targeting" that person. (The statute is silent about acquiring international *radio* communications without intentionally targeting a particular US person, although at the time FISA was passed Congress recognized that Americans do have Fourth Amendment rights in the privacy of the content of such communications.) By repealing or modifying these statutory prohibitions, the bill would suddenly allow the warrantless acquisition of the content of all international telephone, e-mail or other communications sent by any technology to or from Americans so long as it is acquired en masse rather than by *initially* targeting a particular US person's communications.

DOJ Fact Sheet: "For over two decades, the Foreign Intelligence Surveillance Act (FISA), as amended, has served as an important framework in the nation's ability to collect foreign intelligence information, while simultaneously protecting the civil liberties of Americans. FISA provides the legal framework through which the Intelligence Community lawfully collects information about those who pose national security threats to our country. FISA helps those in the Intelligence Community catch spies, international terrorists, and others who seek to do harm to the US, its citizens and its allies."

The Facts about FISA: This law is not just a "tool" or "framework" for electronic surveillance of Americans; it provides "the exclusive" rules for secretly monitoring Americans' conversations and e-mails and searching their homes or offices in the name of foreign intelligence. But the administration deliberately violated these exclusive requirements in the past five years through the NSA's warrantless surveillance program, justified by claims of unchecked presidential power. FISA has not protected Americans' civil liberties, as asserted by the administration, because it was not followed and was treated as optional, rather than constitutionally required.

The secret decision of a single FISA court judge on some part of the NSA program earlier this year does not demonstrate that the law is now being followed. This is because there is no evidence that the ruling requires the individualized warrants for Americans' conversations called for by the Fourth Amendment and FISA. DOJ has refused to provide this assurance and the administration has said the president still has "inherent" power as Commander-in-Chief to monitor Americans outside the strictures of FISA.

FISA's individual warrant and probable cause requirements, when followed, do help protect against national security threats by ensuring that federal agents are properly focused on suspected agents of a foreign power, like al Qaeda, and Americans conspiring with them--by requiring individual warrants approved by a judge. (FISA also does allow for emergency wiretaps and searches of Americans in the US if a secret warrant is sought shortly thereafter.)

DOJ Fact Sheet: "Today, following over a year of coordinated effort among the Intelligence Community and DOJ a bill is being submitted to Congress to request long overdue changes to FISA. The proposed legislation's core objective is to bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interests of persons located in the US. This legislation is important to ensure that FISA continues to serve the nation as a means to protect our country from foreign security threats, while also continuing to protect the valued privacy interests and civil liberties of persons located in the US. The Director of National Intelligence, together with the Attorney General, will work with Congress to ensure enactment of this important proposal to keep America safe."

The Facts about the History of "Updating" FISA: This re-write of FISA is not a technological update to FISA. This proposal is not new and it would severely weaken Americans' privacy protections. These ill-advised proposals were part of the controversial White House-backed bills introduced in the last Congress. And they are still bad ideas this year.

FISA has already been modernized, repeatedly, to take into account changes in technology and threats since 1978. Its provisions have been amended dozens of times, with six major amendments since 9/11, including major changes to "Provide Appropriate Tools to Required to Interrupt and Obstruct Terrorism" in the USA Patriot Act passed by Congress in October 2001.

What has not been done, and what this bill tries to do, is unloose the NSA to acquire countless American conversations and e-mails without any judicial approval or individualized suspicion. This bill would redefine what is subject to judicial orders--creating substantial exceptions to statutory warrant requirements and allowing the government free rein to spy on the content of

Americans' international communications, what Congress sought to prevent after it discovered secret surveillance programs like "Operation Shamrock," where the NSA copied virtually every international telegram cabled to or from people in the US. Contrary to the administration's claims about protecting privacy, the bill actually eliminates key provisions and procedures that "protect the valued privacy interests and civil liberties" of people in the US. It is time to reject the administration's boilerplate claims that it is continuing to protect Americans' privacy when the facts rebut such claims, such as these proposals to delete privacy protections, the years of warrantless wiretapping by the NSA in violation of FISA, and the FBI's documented abuse of the already expansive National Security Letter (NSL) powers.

Now is the time for investigation, not legislation, especially legislation such as this.

DOJ Fact Sheet: "The bill would . . . update the definition of electronic surveillance to account for the sweeping changes in telecommunications technology that have taken place. The proposed legislation is technology neutral. In contrast to the 1978 statute, which contains central provisions that are tied to specific communications technologies, this proposal is not tied to specific technology we have today. That way, as telecommunications technology develops over time--which it surely will do--FISA will not run the risk of becoming out of date."

The Facts about "Tech Neutrality": These "modernization" and "tech neutrality" claims are a Trojan horse, cloaking an administration effort to dramatically cut back FISA's warrant requirements for secretly monitoring Americans' communications. As Congresswoman Jane Harman documented, FISA has been modernized repeatedly since 1978, with major changes since 9/11. This bill does not simply eliminate conceptual distinctions between wire and wireless communications—it rips out major protections for Americans' private communications regardless of the technology used. "Modernization" is an innocuous word being used to distract from the expanded warrantless surveillance the President wants made legal through this bill.

These expansions of unchecked power were first proposed last year, after revelations of the White House's illegal warrantless wiretapping. When the 60 pages of proposed changes to definitions and procedures are scrutinized, it is clear the bill seems design to allow much wider acquisition and mining of conversations and communications of Americans without warrants, by cleverly modifying FISA to exclude them from the warrant requirement through complex changes to the definitions of "electronic surveillance" and "content."

The deletions in the bill appear to allow Americans' international calls and e-mails to be scooped up en masse through any technological means (*i.e., "tech neutral"*) so long as a particular American was not targeted in the *initial* "acquisition" or surveillance. Once Americans' international communications would be thus acquired, without a warrant, the subsequent analysis of private personal or business conversations and data would not count as "electronic surveillance" or require a warrant under the statute or the administration's interpretation of it as evinced by its view of what counts as a "surveillance" device. If the NSA believes you and all the recipients of your communications are in the US, a warrant would still be required. However, as noted above, it is not clear how the administration would treat Americans' e-mail accounts or cell phones under this new language about the government having to "reasonably believe" all communicants are in the US for this protection to apply. It is also unclear how the deletion of the catch-all definition in FISA requiring warrants for the intentional acquisition of "information" by other means--which has been interpreted to include video surveillance--would affect judicial oversight of non-audio surveillance in private homes or buildings in the US. It is absolutely crucial that Congress understand completely the consequences of such changes.

The administration will no doubt assert that its internal foreign intelligence "minimization" rules for information gathered that would not fall under the definition of "electronic surveillance" under

FISA 50 USC 1801(f) or (h) provide additional protections for Americans' privacy, but this is little consolation, given the broad mandate for the widespread sharing of intelligence information. Without an external check on broad claims of need or necessity within the Executive Branch, let alone amid claims of plenary presidential power, there is no way to prevent privacy from taking a back seat to the imperative to gather more and more information into intelligence databases.

A sea change like this requires extensive hearings and investigation. The suggestion that these massive changes should be passed this spring is disrespectful of the democratic process.

DOJ Fact Sheet: "The bill would . . . protect civil liberties and privacy interests and improve our intelligence capabilities by focusing FISA on people located in the US. Revolutions in telecommunications technology have brought within FISA's scope communications that Congress did not intend to be covered—and, as a result, extensive resources are now expended obtaining court approval for acquiring communications that do not directly or substantially involve the privacy interests of Americans. Restoring FISA to its original focus will enhance our intelligence capabilities while allowing the Intelligence Community to devote more resources to protecting the privacy interests of people in the US."

The Facts about the Bill's Changes to Privacy-Related Procedures. There are no, zero, amendments to FISA in this bill that add any privacy provisions and, in fact, the bill expressly deletes long-standing privacy protections for the contents of countless American conversations and communications. If the administration simply wanted to clarify that it need not obtain a FISA warrant for conversations between individuals overseas that can be intercepted in the US (so-called "foreign to foreign" communications that have been rerouted through the US by companies), a simple fix to clarify that has been already proposed by both Senator Feinstein and Congresswoman Harman. This bill goes way beyond that fix. Similarly, if the government does not have enough resources to process FISA warrants for searching Americans' conversations or homes in order to protect both security and privacy, it should endorse the proposal by these Members to provide more resources for the FISA process.

Indeed, the essence of DOJ's claim--that the government is so busy getting FISA court orders that it cannot devote enough resources to protecting Americans' privacy–is belied by the facts. For over five years, the administration simply refused to seek court orders for the wiretaps of Americans that the NSA was illegally conducting, even while the President and his Attorney General reassured the American people their privacy was being protected because court orders were being sought. And, for the past three months, the NSA has been operating under a FISA judge's order that is said to have "creatively" interpreted the law to allow such electronic surveillance of people in the US to go forward, with no commitment that these are individualized warrants. This does not constitute extensive resources being expended to get FISA court approval—and, the judge has likely issued only one or two orders related to the so-called "TSP."

Additionally, although the administration has applied to the FISA court for some wiretaps and physical searches beyond this particular warrantless surveillance program (and the court has rarely denied a request), there is no proof that seeking FISA court approval to secretly wiretap or physically search people in the US adversely affects Americans' privacy. And, if protecting privacy requires more resources than have been allocated, then Congress should authorize more funding, not less privacy. The bill does not "restore" the original intent of FISA; it subverts that intent to protect Americans' privacy. This unwise bill should be shelved.

DOJ Fact Sheet: "The bill would . . . improve the way the US does business with communications providers. The country's communications providers are important partners in the ability of the US Government to protect our national security. The bill includes needed

authority both to protect those carriers when they do comply with lawful requests under FISA, and to enable providers to cooperate with authorized intelligence activities."

The Facts about the Bill's Blanket Immunity: One of the key safeguards built into FISA is the provision that telephone companies and others who intercept Americans' conversations without the judicial warrants required by FISA are potentially criminally liable and may be sued for civil damages. Because FISA provides for secret surveillance, where the targeted individual is unlikely to know of the surveillance, the only check against government violations of the law, is to penalize the communications providers if they do not insist on staying within the law. It is not yet known what the administration told the communications providers that allowed the warrantless NSA surveillance. The administration has refused to provide this information, has blocked the testimony of telecommunications companies and, indeed, is seeking dismissal of the civil lawsuits that are trying to establish responsibility for the illegal surveillance.

This bill seeks to shut down all such inquiry by providing blanket immunity from all civil or criminal penalties for any companies or individuals who may have violated the law, before the facts are even established about their conduct. (The request for immunity, of course, calls into question the administration's repeated claims of complete confidence that the warrantless NSA program was legal. If so, the industry does not need any protection in their lawsuits.)

Moreover, the DOJ "Fact Sheet" omits a key part of the immunity grant. The bill is a full pardon for White House officials and other government agents who knew what FISA required and ignored it anyway. As the White House pointed out in its Statement of Administration Position (SAP) on the Wilson bill last winter (H.R. 5825), this grant of immunity applies to government employees. By the bill's terms, "any person" who provided "assistance" to the intelligence community regarding the warrantless surveillance program, or other classified communications intelligence activities, is immune. This seemingly covers the lawyers in the White House and DOJ who gave their blessing to violations of the law on their theory of presidential power.

The only condition for this blank check immunity from any civil and criminal liability in federal or state courts is that Attorney General Alberto Gonzales certify that the provision of information, facilities or assistance was or even "would have been" intended to protect us, notwithstanding the lack of any ongoing emergency for the past 2,400 plus days. And, FISA already protects companies that comply with court orders by giving them immunity from suit as well as allowing for compensation for lawful assistance. FISA should not be twisted into rewarding the opposite.

It would be impossible to write a broader or more irresponsible grant of immunity. And Congress would be immunizing conduct it has not even investigated yet.

DOJ Fact Sheet: "The bill would . . . streamline the FISA process. Numerous Congressional and Executive Branch reviews of the FISA process have recommended that the FISA process be made more efficient, and the Department of Justice has made major strides in recent years in improving its practices and procedures. The proposal would make several changes to improve further the efficiency of the FISA process, including extending the period of authorization for non-US persons, which will allow the Department and the FISA Court to concentrate more scarce resources to the cases that concern US persons."

The Facts About "Streamlining" FISA Procedures: The bill does contain some provisions that eliminate what the FISA court must be told to authorize a warrant, but in so doing the bill steamrolls, rather than streamlines, the Fourth Amendment's particularity requirements. A far superior approach is providing more resources for improved FISA applications as reflected in the bills by Senator Feinstein (in the bipartisan S. 3877 from the 109th Congress) and Congresswoman Harman (in the strong "LISTEN Act," H.R. 5371). If DOJ were serious about

efficiency and effectiveness rather than simply trying to water down Americans' Fourth Amendment rights under the FISA statute, they would have endorsed these provisions.

Instead, the bill's "summary" provisions seem intended to eliminate privacy safeguards. For example, it is unclear what the administration intends to accomplish by requiring a "summary" description of the place to be searched with a warrant rather than a "detailed" description of the home or business in the US to be physically searched. The requirement of a detailed description is consistent with the Fourth Amendment's command that warrants "particularly" describe "the place to be searched, and the persons or things to be seized." Yet the administration asserts in essence that requiring such particularity or detail detracts from privacy; to the contrary, such particularity helps ensure that the right person's home or office is searched and minimizes the chance that innocent people will have their private domain secretly invaded. (The bill also contains a peculiar and troubling change to allow warrants to search a home *before* it is owned or occupied by a suspected terrorist, which by definition is then a place occupied by an innocent resident whose drawers and papers should not be searched without the probable cause required by FISA and the Fourth Amendment. This is another example of the wish-list approach of this bill.)

The DOJ "Fact Sheet" omits other ways in which its streamlining diminishes Americans' privacy protections. The bill would substantially extend the period of secret surveillance allowed with a warrant. It would allow round-the-clock surveillance of Americans in one-year increments upon renewal of an order, with no judicial supervision during that time about whether the wiretap was even productive for gathering foreign intelligence.

DOJ Fact Sheet: "The bill . . . reflects today's national security threats. The bill seeks to update FISA to reflect today's national security threats. One of those threats is the proliferation of weapons of mass destruction. This legislation will allow the Intelligence Community to obtain FISA authority to better protect the nation against proliferators."

The Facts about WMD in this Context. There is no doubt the proliferation of unconventional weapons is dangerous, but it is unclear why the current definitions and provisions in FISA do not already provide ample authority to wiretap anyone in the US who is conspiring to develop or use such weapons illegally for terrorism or sabotage. FISA expressly allows for the wiretapping of suspected agents of a foreign power, regardless of the mechanism used. To borrow a page from DOJ, FISA is already "weapons neutral"--FISA should not start listing weapons in any way that would make such a list seem exclusive or too narrow. FISA should remain focused on the nature and status of the people under surveillance rather than listing specific weapons.

The administration gives no explanation about what difference it would make to add the proposed language. Is it meant to allow the secret surveillance of every foreign scientist working on nuclear energy in this country? Or are the WMD definitions so broad that possession of common items such as pool chemicals or gunpowder--precursors that are lawful for Americans to possess--could be used as a basis for surveillance? Or is the intent simply a political strategy to try to claim that anyone who dares to oppose this package of bad ideas is refusing to prevent WMD terrorism? That would be a wrong claim, in every sense of the word.

DOJ Fact Sheet: "The bill would . . . add an additional definition of an agent of a foreign power for non-US persons whom the Government believes possess significant intelligence information, but whose relationship to a foreign power is unclear. This proposed change would apply only to non-US persons in the US, and collection of information from such an individual would be subject to the approval of the FISA Court."

The Facts about "Agent of a Foreign Power": Congress already provided the administration with a very controversial "lone wolf" amendment, in the President's first term, to allow wiretaps of non-US persons in the US who are plotting international terrorism unconnected to a foreign power. *See* Section 6001 of the Intelligence Reform and Terrorism Prevention Act, 75 Pub. L. 108-458, 118 Stat. 3742 (2004) (subject to the sunset provisions). Thus, Congress has already addressed potential foreign terrorists "whose relationship to a foreign power is unclear."

This bill would allow extremely widespread surveillance of any non-green card holder in this country, not on any suspicion of terrorism, espionage or any crime at all, but simply on the basis that the individual might know "foreign intelligence information" of interest to the government. Such information is not limited to information about sabotage or international terrorism but includes broad information about "the conduct of US foreign affairs" or "defense." The fact that a warrant would be required does not provide much protection because the statute would be changed to permit such surveillance, meaning it provides for the court to legally approve it.

And, in our global economy, many well known companies, even news services, in the US do not count as US persons under FISA's definitions because of the location of their incorporation—even if they employ or do business here with numerous Americans. This new provision would open such companies as well as foreign nationals to secret, round-the-clock monitoring of phone conversations or e-mails, when there is no suspicion of wrongdoing. The person or business might not even know they possess foreign intelligence information and might not actually possess any such information. Such surveillance would undoubtedly intercept countless innocent communications, including numerous conversations with Americans, including employees of such companies. The bill does not contain any significant protection against agents listening to, keeping and using such communications.

Other Facts Ignored in DOJ Fact Sheet: The bill also attempts to short-circuit existing judicial review of the warrantless NSA surveillance program. In addition to the grant of immunity discussed above, the bill would strip federal and state courts, except the FISA court, of the power to hear existing claims against that program or any other classified intelligence activities. That is, it would prevent fairly and randomly chosen judges from state and federal courts with pending or future constitutional or state privacy claims from considering the merits of these claims. The bill would force such claims to go before the FISA court, constituted of judges picked by the Chief Justice, for largely secret proceedings to adjudicate the constitutional rights of Americans. And, under the terms of these provisions, if the government sought access to the judge without the other party present, the court would be required to grant such requests.

The administration's bill also replaces the narrow exception to the warrant requirement for embassies in the US with broader authority to acquire communications in the US without a court order, simply based on the Attorney General's certification or directive. For example, section 102 of FISA would be changed to eliminate the narrow exception that a warrant is not required if the surveillance is directed "solely" at the communications of foreign governments here, and it deletes the bar on such warrantless surveillance even when there is a "substantial likelihood" Americans' conversations will be swept in. That is, the Attorney General could order warrantless surveillance directed toward a foreign government here even if such surveillance was likely to sweep in Americans' conversations. And the bill strikes the statutory protections for American conversations obtained inadvertently without warrants, by eliminating FISA's requirement in 50 USC 1801(h)(4) that such conversations be deleted within three days of acquisition unless the government obtains a court order or there is a threat to life or bodily injury. The bill would also add new sections, 102A-C, to allow "acquisition of information" without a court order relating to a person believed to be outside the US. These and changes to the rules for warrants proposed in the administration's bill should be thoroughly evaluated.

Hearing of the

United States Senate

Select Committee on Intelligence

Tuesday, May1, 2007

Testimony of Suzanne E. Spaulding

I want to thank the Senate Select Committee on Intelligence for this opportunity to submit testimony in the context of the May 1, 2007, hearing on the Foreign Intelligence Surveillance Act (FISA).

I'd like to begin by emphasizing that I have spent over twenty years working on efforts to combat terrorism, including serving as General Counsel and Deputy Staff Director of this committee in the mid-90s. Over those two decades, in my work at the Central Intelligence Agency, at both the House and Senate intelligence oversight committees, and as Executive Director of two different commissions on terrorism and weapons of mass destruction, I developed a strong sense of the seriousness of the national security challenges that we face and deep respect for the men and women in our national security agencies who work so hard to keep our nation safe.

We owe it to those professionals to ensure that they have the tools they need to do their job; tools that reflect the ways in which advances in technology have changed the nature of the threat and our capacity to meet it. Equally important, they deserve to have careful and clear guidance on just what it is that we want them to do on our behalf -- and how we want them to do it. Clear rules and careful oversight provide essential protections for those on the front lines of our national security efforts.

This is particularly critical with regard to the collection and exploitation of intelligence related to threats inside the United States, which I will refer to as domestic intelligence.[1] The attacks of 9/11 revealed a vulnerability at home that led to a dramatic increase in domestic intelligence activity. The Federal Bureau of Investigation's priorities turned 180 degrees, as it was pressed to place domestic intelligence collection at the forefront rather than criminal law enforcement. But the FBI is not the only entity engaged in domestic intelligence. The Central Intelligence Agency, National Security Agency, Department of Defense, Department of Homeland Security, and state and local law enforcement are among the many entities gathering intelligence inside the US. The collection of information on the movement, communications, and activity of any international terrorists that may be targeting and operating in the US presents unique challenges, both to effective intelligence and to appropriate protections against unwarranted government intrusion.

Unfortunately, the legal framework governing this intelligence activity has come to resemble a Rube Goldberg contraption rather than the coherent foundation we expect and need from our laws. The rules that govern domestic intelligence collection are scattered throughout the US Code and a multitude of internal agency policies, guidelines, and directives, developed piecemeal over time, often adopted quickly in response to scandal or crisis and sometimes in secret.

Rather than continuing this pattern, I urge Congress not to consider the kind of dramatic and far-reaching overhaul of FISA that has been proposed by the

[1] Included in this concept of domestic intelligence is any intelligence that involves a domestic component, such as the interception of communications between someone in the US and someone outside the country. This does not pre-suppose how that intelligence ultimately should be treated but acknowledges that it raises potentially different issues than intelligence involving purely foreign components.

Administration without first undertaking a comprehensive review of domestic intelligence.

A Joint Inquiry or Task Force could be established by the Senate leadership, with representation from the most relevant committees (Intelligence, Judiciary, Armed Services, and Homeland Security and Government Affairs), to carefully examine the nature of the threat inside the US and the most effective strategies for countering it. Then Congress, and the American public, can consider whether we have the appropriate institutional and legal framework for ensuring that we have the intelligence necessary to implement those strategies, with adequate safeguards and oversight.

The various authorities for gathering information inside the United States, including the authorities in FISA, need to be considered and understood in relation to each other, not in isolation. For example, how does the authority proposed for a new FISA section 102A relate to the various current authorities for obtaining or reviewing records, such as national security letters, section 215 of FISA, the pen register/trap and trace authorities in FISA, and the counterparts to these in the criminal context, as well as other law enforcement tools such as grand juries and material witness statutes? And how do these techniques relate to more intrusive investigative and intelligence tools?

Executive Order 12333, echoed in FISA, calls for using the "least intrusive collection techniques feasible." The appropriateness of using electronic surveillance to eavesdrop on Americans should be considered in light of other, less intrusive techniques that might be available to establish, for example, whether a phone number belongs to a suspected terrorist or the pizza delivery shop. It's not the "all or nothing" proposition often portrayed in some of the debates.

The recent report by the Inspector General on the misuse of national security letter authority found, similarly, that while Attorney General guidelines on National Security Investigations also cite the requirement to use the least intrusive techniques feasible, there is not sufficient guidance on how to apply that in the national security letter context or in conjunction with other available collection techniques.

Many of these authorities, moreover, have been amended since 9/11 in ways that seem to permit the gathering of vast amounts of information that could then be used for purposes of data mining. Some kinds of data mining could provide essential national security capabilities that the government should be actively researching and developing. Unfortunately, equally essential public discussion and debate about appropriate policies to govern data mining implementation were cut short by the public reaction to early proposals such as Total Information Awareness. Thus, the legal authority to collect the information continued to expand without adequate consideration of safeguards to ensure appropriate use of that information. Some of the proposed changes to FISA would further exacerbate this trend. This needs to be considered more comprehensively.

Additionally, while there has been much public debate about the role of the FBI, there has been very little discussion about the domestic intelligence activities of other agencies such as CIA and the Defense Department. For example, executive branch lawyers assert that the Global War on Terrorism (GWOT) is a war in the full legal sense and the battlefield is wherever suspected terrorists are or might be in the future. Intelligence collection is a key aspect of preparing the battlefield and an important aspect of DOD's homeland defense mission. Moreover, section 1681v of the Fair Credit Reporting Act allows any agency engaged in counter-terrorism analysis, including presumably DOD, to demand consumer reports on US citizens and others. Congress needs to understand exactly what DOD is doing inside the United States

and promote a robust and informed discussion about what it is we want them to be doing. Under what legal authorities is it operating? Should DOD meet its own intelligence requirements inside the United States or should the FBI or some other entity be responsible for gathering information for all those who need it, including DOD?

Congress should undertake this comprehensive consideration of domestic intelligence with an eye toward the future but informed by the past and present. Until Congress fully understands precisely what has and is being done in terms of the collection and exploitation of intelligence related to activities inside the US, by all national security agencies, it cannot wisely anticipate the needs and potential problems going forward.

This applies to the proposed changes to FISA, as well. Congress must be certain that it has been fully informed about the details of the Terrorist Surveillance Program and any other surveillance programs or activities initiated after 9/11, not just in their current form but in the very earliest stages. Understanding how the law operates in times of crisis and stress is key to understanding how it might need to be strengthened or adjusted.

A fundamental concern with the FISA overhaul proposed in this legislation is that the government has not adequately explained to the American public, and perhaps even to Congress, precisely why these changes are necessary and justified. It is reasonable to assume that some changes to FISA— in addition to all of the changes already made since 9/11-- might be appropriate to address changes in technology. For example, communications between non-USPs outside the United States are not subject to FISA. They should not suddenly fall within FISA's scope simply because they happen to transit the US.

However, many of the changes to FISA proposed in this legislation are troubling. I will highlight a few of the most significant in my testimony today.

Among the changes of greatest concern are those made to the definitions of terms used throughout the FISA statute. Changing the meaning of those terms has potentially far-reaching consequences that are not always readily apparent without a detailed analysis of each place in the statute where the term is used. In addition, FISA definitions inform the use of these terms in numerous other contexts, such as intelligence directives and policies.

Changes that raise particularly significant concerns include:

Electronic surveillance: The safeguards of FISA with regard to electronic communications apply almost exclusively to "electronic surveillance." The bill appears to exclude from that definition, and thereby allow warrantless interception of, calls or emails of persons, including US citizens, inside the US who are communicating with persons, again including US citizens, outside the US, so long as the government is not directing the intercepts at a *known* US person (USP) inside the US. Note that this exemption from FISA would not be limited to communications in which a suspected terrorist or other agent of a foreign power was at one end of the call.

Surveillance devices: The changes would also seem to allow, without a warrant, broader use of a wide range of surveillance devices against US citizens and others. Part of the current definition of "electronic surveillance" includes installation of *any* surveillance device (e.g., camera, infrared sensor, etc.) inside the US under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes. Under the proposed amendments, such surveillance devices would only be covered by FISA if they are

intentionally directed at a particular, known USP. As a result, conducting such technical surveillance, even under circumstances where there is a reasonable expectation of privacy and a warrant would be required for law enforcement purposes--such as in a private meeting facility or place of worship--would now seem to be defined-out of FISA, so long as the government is not targeting a particular, known US person.

Agent of a Foreign Power: The bill would broaden this definition to include any non-US person who possesses, or is expected to receive, "foreign intelligence information," a term that was earlier amended to include any information that relates to "the ability of the United States to protect against actual or potential attack." The person possessing the information does not need to have any connection with terrorist activities, let alone a terrorist group or other foreign power. The bill does not require that the person provide this information to anyone or even ever contemplate giving it to anyone; merely possessing the information makes you an agent of a foreign power. Vast categories of privately held information that have nothing directly to do with terrorist attacks, including information about co-workers or classmates, or building blueprints, might be determined by the government to be related to the ability to protect against a potential attack. Any non-USP the government decided possessed such information, even if they worked for a US company or US newspaper, would be an agent of a foreign power and thus potentially subject to having the government not only seize the information but intercept their communications or secretly search their premises. Since even non-USPs are guaranteed the protections of the Fourth Amendment, this change could raise serious concerns about the continued constitutionality of FISA.

Weapons of Mass Destruction. The definition of an agent of a foreign power is further broadened to include persons engaged in the development of weapons of mass destruction (WMD). It is not clear why existing laws, including FISA provisions related to preparations for sabotage, etc., are not adequate. Moreover, the definition of WMD is broad and vague. It includes "any destructive device"-- not just chemical, biological, nuclear, or radiological devices-- intended or *capable of* killing or seriously injuring "*a significant number of people.*" Another part of the definition includes any weapons intended to cause death or injury through release of toxic chemicals, which could cover the assassination of a single individual with a toxic umbrella tip. And there is no requirement for any foreign connection, since even the definition of a foreign power would be amended to include any "group engaged in the proliferation of weapons of mass destruction." Again, this moves still further away from the original justification, articulated by the courts and Congress, for the unique, secret intelligence authority provided in FISA.

Minimization Procedures: The proposed legislation would significantly alter the safeguards currently applicable to surveillance authorized by the Attorney General, while at the same time expanding that unilateral authority far beyond its initial scope of simply foreign power to foreign power communications. Under current law, if surveillance is conducted pursuant to AG authorization rather than a warrant from a FISA judge, no contents of any communication to which a USP is a party can be disclosed, disseminated, or used for any purpose or retained for more than 72 hours without getting a court order, unless the AG determines that the information indicates a threat of death or serious bodily harm. Concern about ensuring that electronic surveillance authorized unilaterally by the AG could not be used to gather information about USPs was so strong when FISA was enacted that even the mere existence of

such a communication (included in the current definition of "contents") was included in this restriction. This entire section is deleted in the proposed bill.

Instead, under the proposed legislation, broad unilateral AG authority would be statutorily subject only the weaker procedures that currently apply in instances where a FISA judge has reviewed an application to ensure that the target is a foreign power or an agent of a foreign power. These simply require procedures reasonably designed to "minimize" the acquisition and retention of USP information "consistent with the need to obtain, produce, and disseminate foreign intelligence information." The AG is also freed from the requirement to certify that "there is no substantial likelihood" that the surveillance will acquire a communication to which a USP is a party. This loosening of restrictions with regard to US person conversations is disturbingly consistent with, and exacerbated by, proposed changes in Section 102 that expand the AG's power to authorize warrantless surveillance of conversations involving USPs, so long as the target is a foreign power.

Contents: The proposal would eliminate from the definition of "contents" information about the identities of the parties and the existence of the communication. Instead, it would be limited it to the "substance, purport, or meaning" of the communication. The argument for this change is that it conforms the FISA definition to the one contained in the statute pertaining to communications intercepts in criminal investigations and will conform the FISA pen register/trap-and-trace authorities with their counterparts in the criminal context. Congress needs to ensure that it fully understands the potential impact of this change.

First, this change does not just affect pen register and trap-and-trace authority. The term "contents" informs other key definitions and authorities in FISA. Under the new definition of electronic surveillance, for example, even the interception of

purely domestic calls or emails would not be covered under FISA so long as the government was not intentionally acquiring the "contents" of those calls or targeting a particular, known USP. This would seem to allow the interception of purely domestic calls if the government only "acquired" information such as the gender of the parties, the tone of voice, the language spoken, etc.

As noted earlier, FISA's current broader definition of "contents" reflects the particular sensitivity of secretly intercepting calls of US citizens in a context where the normal safeguards and transparency built into our criminal system do not apply. Moreover, it is not clear what impact changing this definition might have in other contexts, such as NSA's ability to search its databases for USP names. At a minimum, Congress should consider only applying this change to the pen register and trap-and-trace provisions rather than the entire statute.

There are many more potential problems with the changes in this legislation. These include, in addition to the dramatic expansion of unilateral AG authority, expanding the role of FISA judges and the Foreign Intelligence Surveillance Court of Review in a way that reduces the check currently provided by the knowledge that their decisions might be reviewed by a regular Article III judge, and the vast expansion of certifying authority beyond the ranks of politically-accountable Presidential appointees to anyone in the executive branch.

The proposed extremely broad blanket immunity for the telecommunication companies and others also deserves particularly careful examination. It's not clear why this is needed. In an area such as this, where the normal safeguards of transparency are lacking, requiring communication providers to at least get a certification that the request to hand over customer information or allow

communication intercepts is legal serves as an important potential deterrent to abusive behavior by the government. Congress needs to fully understand what past activities would be immunized before adopting such a wide-ranging provision.

FISA is the primary statute governing domestic intelligence collection. Rather than attempt to fix this proposal and guess at what might really be needed to meet today's challenges, Congress should take the time to ensure they understand the full context in which these changes are being sought. This includes the problems that have prompted them, particularly as these relate to current and past intelligence activities and the changing nature of the threat, as well as how these new authorities, definitions, and procedures would relate to all of the other national security and law enforcement tools available to the government.

Statement for the Record
K. A. Taipale, Executive Director
Center for Advanced Studies in Science & Technology Policy

Foreign Intelligence Surveillance Modernization: Reconciling Signals Intelligence Activity with Targeted Wiretapping

Senate Select Committee on Intelligence Hearing on
The Foreign Intelligence Surveillance Modernization Act of 2007

May 1, 2007

The Center for Advanced Studies in Science and Technology Policy, an independent, non-partisan research organization focused on information, technology, and national security policy, has long advocated that the Foreign Intelligence Surveillance Act of 1978 ("FISA") be carefully amended to provide an updated statutory mechanism so that legitimate foreign intelligence and national security needs can be met while still protecting privacy and civil liberties. [1]

On April 13, 2007 the Director of National Intelligence submitted legislation to Congress (Title IV of the Fiscal Year 2008 Intelligence Authorization Act, The Foreign Intelligence Surveillance Modernization Act of 2007) ("FISMA") requesting that FISA be amended "to bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interests of persons located in the United States."

We are pleased to submit this statement discussing certain issues relating to FISA modernization in connection with the Senate Select Committee on Intelligence hearing to consider this legislation. We focus in this statement primarily on the issues relating to the use of signals intelligence activities, including those targeted against legitimate foreign intelligence targets not subject to FISA, when those activities may have significant impact on U.S. persons because they involve communications to or from the United States.

---

[1] *See, e.g.*, K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, N.Y.U. REV. L. & SECURITY, NO. VII SUPL. BULL. ON L. & SEC.: THE NSA AND THE WAR ON TERROR (Spring 2006) at *http://whisperingwires.info/*; and K. A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128 *(Spring 2007) available at* http://ssrn.com/abstract=959927.

Introduction.

FISA should be amended as it is no longer adequate either to enable legitimate foreign intelligence activity or to protect privacy and civil liberties. FISA simply did not anticipate the nature of the current threat to national security from transnational terrorism, nor did it anticipate the development of global communication networks or advanced technical methods for intelligence gathering. Because of technology developments unanticipated in 1978, FISA warrant and procedural requirements are now being triggered in circumstances not originally intended to be covered by FISA and for which such procedures were not designed and are not well-suited. [2]

The current public debate over FISA modernization is needlessly polarized because of a failure to adequately address directly the fundamental political and policy challenges resulting from this blurring of the previously clear demarcation between reactive law enforcement-derived policies governing the use of targeted "wiretaps" to monitor communications of known persons in the United States pursuant to warrants issued on a prior showing of probable cause on the one hand, and preemptive national security strategies that rely on "signals intelligence" (activity not directed at targeted individuals in the United States but rather at finding information with foreign intelligence value for counterterrorism or counter-proliferation purposes from monitoring foreign intelligence channels or targets, including their international communications to and from the United States) to identify and preempt unknown threats on the other.

As discussed in the following section, when FISA was enacted it was intended only to cover targeted domestic surveillance for foreign intelligence purposes. In keeping with this intent, the administration has proposed amending FISA to exclude non-targeted signals intelligence activity from the definition of "electronic surveillance." In addition, the Attorney General would be given authority to approve "the acquisition of foreign intelligence information concerning persons reasonably believed to be outside of the United States" from "communication service providers" (provided that such acquisition did not constitute the newly defined "electronic surveillance").

The effect of these changes would be to exclude from FISA warrant requirements foreign signals intelligence activities directed at legitimate foreign intelligence targets outside of the United States, including their communications to and from the United States, and, if authorized by the Attorney General, additional foreign intelligence information relating to these targets obtained from domestic communication providers. Information obtained through these activities that concerned U.S. persons would be subject to minimization procedures but would be available for use to support FISA warrant applications to target such U.S. persons if the information had significant foreign intelligence value.

---

[2] See generally, *id.*

We have previously advocated that FISA be amended (1) to provide an explicit statutory authorization and oversight mechanism for programmatically approving certain foreign signal intelligence activity that may substantially affect U.S. persons, and (2) to provide an explicit procedure for using information derived from such signals intelligence activity as a predicate in appropriate cases for subsequent targeted "wiretap" surveillance pursuant to FISA warrant procedures.

While the administration's proposed amendments address the same problems with FISA that we have previously identified—and we generally support the effort to modernize FISA—we would prefer to see an additional statutory authorization or oversight mechanism specifically designed to provide additional privacy and civil liberties protection (through specific authorities, oversight, or review) for situations in which either programmatic or foreign-targeted signals intelligence activities are likely to have a significant impact on persons in the United States. Thus, we urge that the Committee, the Congress, and the administration consider the issues discussed below.

Changes in technology challenge the existing FISA framework.

When FISA was enacted in 1978 it was intended only to cover targeted foreign intelligence interceptions of domestic communications within the United States. It was specifically not intended to cover non-targeted signals intelligence activities to collect foreign intelligence (nor communications intercepted incidental to surveillance targeting a foreign intelligence target not itself subject to FISA). The exclusion of National Security Agency ("NSA") signals intelligence activities, including activities directed at intercepting international communications, was explicitly acknowledged at the time:

> Because of the different nature of government operations to collect foreign intelligence by intercepting international communications—a process described as the interception of signals and the processing of those signals by techniques which sort and analyze the signals to reject those that are inappropriate or unnecessary—that use of electronic surveillance is not addressed in this bill. [3]

The legislative history is replete with references acknowledging Congressional awareness of ongoing signals intelligence activities relating to international communications then being conducted by the NSA (including "sweeping" interceptions of communications where one end was in the United States) and makes it clear that it was not contemplated that such activity was to be subject to FISA warrant or procedural requirements. [4]

---

[3] *Foreign Intelligence Surveillance Act, Hearing before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary, United States Senate*, 94th Congress, at 11 (March 29-30, 1976) (Statement of the Hon. Edward H. Levi, Attorney General of the United States).

[4] For example, Attorney General Levi testified that "[w]here there is a radio communication [including the microwave portion of a wire transmission, *see* note 5 *infra*] of an international kind which is picked up in some kind of sweeping operation or some other kind of operation; that is beyond the scope of [FISA]." Statement, *supra* note 3 at 15. And further, "I think the fact of the matter is that this bill does not provide for facts and circumstances, which I specifically mentioned, namely the transatlantic kinds of sweeping overhearing, with which members of this committee, I am sure, are somewhat familiar. *Id.* at 17.

Indeed, the differing statutory standards enacted in FISA for "wire" and "radio" intercepts, and for interceptions conducted "within the United States" and abroad, were designed specifically as statutory mechanisms to preserve the distinction between signals intelligence not subject to FISA and targeted domestic activity that was to be its domain.[5]

Thirty years ago when FISA was being drafted these technical distinctions based on place or method served to distinguish signals intelligence from targeted "wiretapping" and made perfect sense given the then prevalent practices and technologies. Signals intelligence activities at that time were primarily being conducted by foreign intelligence agencies like the NSA through interception of satellite or microwave transmissions (i.e., "radio") that could be intercepted from abroad (even when they had one "end" in the United States), and targeted interceptions of specific communications of known persons were generally being conducted by law enforcement or counterintelligence agencies like the FBI using a "wiretap or microphone" on circuit-based "wire" transmissions within the United States. FISA was intended to cover the latter and designed to exclude the former.[6]

And, at a subsequent FISA hearing in the House, when asked by Congressman Railsback to give a specific example of an activity that was not within the scope of FISA, the Attorney General stated: "... there is a kind of sweeping operation by the NSA which is dealing with international communications not covered here. And that is uncovered in this bill." *Foreign Intelligence Surveillance Act, House Subcommittee on Courts, Civil Liberties, and the Administration of Justice of the Committee on the Judiciary*, 94th Congress, at 91 (June 2, 1976) (Statement of Edward H. Levi, Attorney General of the United States).

5 This intention is explicitly acknowledged in the legislative history:

> The reason for excepting from the definition of "electronic surveillance" the acquisition of international radio transmissions, including international wire communications [i.e., international telephone calls] when acquired by intercepting radio transmission [i.e., microwave transmission thereof] when not accomplished by targeting a particular United States person in the United States, is to exempt from the procedures of the bill certain signals intelligence activities of the National Security Agency.

S. REP. NO. 95-604, 95th Cong., at 34 (1977).

The intentionality of this distinction between "wiretap" activities and signals intelligence activities is further evidenced by the way FISA explicitly defines "wire transmission" as "any communication *while it is being carried by a wire, cable, or other like connection*" (50 U.S.C. §1801(l), emphasis added). This qualifier—"*while it is carried by*"— is necessary because 18 U.S.C. §2510(1) defines "wire transmission" as any communication "made in whole or part" through wire facilities. The Senate Report explains the need for this qualification by noting that "most telephonic and telegraphic communications are transmitted at least in part by microwave transmission" and that FISA is only intended to apply to "those surveillance practices which are effected by tapping into the wire over which the communication is being transmitted" within the United States or where the interception "targets" a U.S. person or intentionally intercepts a radio transmission in which the sender and all of the intended recipients are in the United States (i.e., purely domestic microwave communications). S. REP. NO. 95-604 at 33. Thus, FISA was crafted with some intentional definitional complexity specifically to exclude non-targeted interception of international communications, including those with one end in the United States.

6 Attorney General Levi testified:

Unfortunately, these outdated technical distinctions are now inadequate to address certain technology developments that have occurred since the enactment of FISA, including the transition from circuit-based communications to packet-based communications; the globalization of communications infrastructure; and the development of automated monitoring techniques, including data mining and traffic analysis.

Because of these technology developments, much legitimate foreign signals intelligence activity directed at finding signals of interest (that is, activity not directed at targeted individuals in the United States but rather at finding information with foreign intelligence value for counterterrorism or counter-proliferation purposes from monitoring legitimate foreign intelligence channels or targets, including their international communications to and from the United States) can no longer be conducted within the framework envisioned by FISA. Activities previously accomplished by radio interceptions or conducted abroad (and intentionally excluded from FISA procedures) are increasingly only possible through interceptions conducted at communication switches within the United States (including "transit intercepts" of wholly foreign communications) or at switches or fiber optic cable repeaters that carry significant U.S. person or domestic traffic as well (resulting in the "substantial likelihood" of collateral intercepts), thus, potentially triggering FISA and its procedural requirements in circumstances that were not contemplated at enactment.

A detailed discussion of these technology developments—including how they interact with FISA and how FISA procedures are being triggered in circumstances such as transit intercepts, collateral intercepts, and through automated signals intelligence processing activities that FISA was never intended to cover (and for which current FISA warrant procedures are ill-suited)—is included in my recent article, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, published in the Yale Journal of Law and Technology, a copy of which is attached and incorporated herein by reference. [7]

Preemption, not technology, poses the more difficult policy problem.

The fundamental challenge to existing law and policy, however, is not technological—if it were, resolution might be more easily accomplished. The real challenge arises from the need to pursue preemptive strategies against certain potentially catastrophic threats from

---

> But, as I have pointed out, the bill is by its definition limited to the interception within the United States by electronic surveillance, as defined, of foreign intelligence information. The bill does not purport to cover the interceptions, other than by the use within the United States of devices such as wiretaps or microphones, of international communications.

Levi, *supra* note 3, at 12-13. And, *see* note 5 *supra*.

[7] K. A. Taipale, *The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance*, 9 YALE J. L. & TECH. 128 *(Spring 2007) available at* http://ssrn.com/abstract=959927.

transnational terrorism and nuclear weapons proliferation that in part necessitate using electronic surveillance methods that were not originally intended to be covered by FISA or related warrant procedures (and that don't easily lend themselves to such practices) but that increasingly affect the privacy and civil liberties interests of persons in the United States. [8]

The challenge is in crafting a new framework—one that is both enabling of legitimate foreign intelligence activities and yet protective of privacy and civil liberties—to govern the use of signals intelligence methods (particularly, those methods that were originally not intended to be subject to FISA and for which the existing FISA procedures are not well-suited) against new national security threats when these uses increasingly impact the same privacy and civil liberties interests that FISA *was* originally intended to address.

The policy conundrum is in reconciling the rigid law enforcement-derived policies and procedures intended to govern the use of electronic surveillance technologies to monitor the activities of known subjects with the more amorphous foreign intelligence and national security strategies needed to identify previously unknown threats (in order to develop the kind of actionable intelligence necessary for preemption). These activities were previously subject to disparate and often conflicting policy regimes—the former subject to formal judicial warrant procedures under FISA and the latter at the sole discretion of the executive with little oversight or review.

The administration's proposals: exclude signals intelligence from FISA

The proposed Foreign Intelligence Surveillance Modernization Act of 2007 ("FISMA") would amend FISA to exclude most foreign and international signals intelligence activity from triggering FISA warrant requirements by simplifying the definition of "electronic surveillance" for purposes of the statute to interceptions (1) intentionally targeting a particular, known person reasonably believed to be in the United States, or (2) intentionally acquiring the contents of communications when all parties are reasonably believed to be in the United States. The effect of these changes would be to exclude any non-targeted interception of international communications from FISA or its warrant requirements even if one party to the communication was in the United States. [9]

Although it can be argued persuasively that such a proposal merely updates—in a way no longer dependent on outdated technical distinctions—the original legislative intention for FISA to not cover these kinds of activities, in our view it fails to acknowledge the political reality that certain of these "foreign" activities increasingly infringe on the

---

[8] It is beyond the scope of these comments to delineate precisely where the line should be drawn between threats to national security that require a preemptive approach and those that remain amenable to traditional reactive law enforcement methods. However, it is axiomatic that national security assets, including foreign intelligence surveillance capabilities, should be employed only against true threats to national security and not for general law enforcement or social control purposes.

[9] As discussed below, another effect of this definitional change would be to exclude from FISA non-targeted collection of non-content or "transactional" information about communications.

legitimate privacy expectations of persons in the U.S. in ways and degrees not previously contemplated and, therefore, as a *policy* matter, certain of these activities with the potential for significant domestic impact may now require some form of explicit statutory authorization and oversight mechanism external to the executive branch to create political consensus, reassure the public, and provide democratic accountability. [10]

Thus, regardless of whether the executive indeed has inherent authority to conduct foreign intelligence surveillance activities—including those that intercept international communications to and from the United States—without such explicit statutory authority or oversight, our system of government works best, and public confidence is best maintained, only when the branches of government work together in consensus and the broad parameters of procedural due process protections are publicly debated and agreed.[11]

In discussing the intentional exclusion of NSA signals intelligence activities from FISA, the 1977 Senate Report No. 95-604 at 64 states:

> The activities of the NSA pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the Committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the NSA and the surveillance of Americans abroad raises problems best left to separate legislation.

Because of the difficulties in continuing to maintain separate policy regimes, particularly for foreign intelligence activities outside of FISA that may substantially affect the privacy and civil liberties interests of large numbers of persons in the U.S. in ways not previously contemplated,[12] it may be time to address these conceptual and technical difficulties

---

[10] It should be noted that FISA itself was "not a response to some presumed constitutional requirement of a judicial warrant as a condition of the legality of surveillance undertaken for foreign intelligence purposes. Such a requirement has not been the holding of the courts ..." rather, FISA was enacted to bring consistency to fragmented legislation, judicial decisions, and administrative action and practice in these areas. FISA was a political compromise in which the inherent but undefined executive power to conduct foreign intelligence surveillance explicitly acknowledged by the courts was "augmented" by legislation in return for subjecting domestic foreign intelligence surveillance to a statutory regime, including statutory warrant procedures. *See* Levi, *supra* note 3, at 8-9, 16.

[11] I take no position in these comments on the important constitutional issue of whether the executive has sole, primary, or shared authority to conduct foreign intelligence activities pursuant to his commander-in-chief or foreign affairs powers. My suggestion for seeking legislative authority for programmatic approval of certain foreign intelligence activities with a substantial impact on U.S. persons, as is implicit in these comments, is based on my view that it is advisable for policy reason to put such activity on an explicit statutory foundation in order to engender the broadest possible political, judicial, and public support for legitimate and necessary foreign intelligence activities vital to the national security of the United States.

[12] It should be noted that NSA foreign signals intelligence activities were likely to affect many fewer persons in the U.S. thirty years ago when FISA was enacted than in today's globalized economy and communications networks—both because more people in the U.S. are now likely to be engaged in international communications but also because it is increasingly difficult to actually differentiate foreign,

directly rather than to ignore them by simply excluding all such activity from any legislative reach. [13]

Requiring traditional FISA warrants for signals intelligence is unworkable.

Many critics of the administration's proposed amendments concede that changes in technology have undermined the existing FISA framework. [14] However, they argue that rather than excluding non-targeted or foreign intelligence activities from FISA as proposed by the administration, that these technology developments justify extending existing FISA warrant requirements to all electronic surveillance activities in which U.S. person or domestic communications are likely to be intercepted, even if no U.S. person or communication is targeted and the communication is merely acquired incidental to the targeting of legitimate foreign intelligence targets. But, in doing so they ignore the fundamentally different requirements and circumstances of non-targeted or foreign signals intelligence and targeted domestic wiretaps. [15]

If the existing FISA warrant procedures were to be strictly applied to all foreign intelligence activities then no useful signals intelligence activity of any kind would be possible—there would simply be no procedure under which electronic signals intelligence could be employed to uncover unknown connections or threats from persons in the United States communicating or conspiring with known al Qa'ida or affiliated operatives. Such an outcome would, of course, have significant national security ramifications.

In any case, there is no constitutional requirement for warrants in these circumstances.[16] For a discussion of the relevant constitutional constrains, see *Hearing on Modernizing the*

---

international, and domestic communications within a globalized packet-based communication network in which traffic is routed dynamically and where local addressing information can be used globally. See *The Ear of Dionysus*, *supra* note 7, at 143-145, 146-147, 146 n.50, and 147 n.51.

[13] We are not advocating that all foreign intelligence surveillance activity come under a statutory scheme—indeed, there would be significant separation of powers issues involved if it did—but only that a mechanism to approve specific programs or kinds of signal intelligence activity where there is a substantial likelihood of acquiring the contents of U.S. persons be considered for policy reasons in order to garner the widest possible political, judicial, and public support for legitimate foreign intelligence activities.

[14] *See, e.g.*, Center for Democracy & Technology, *Modernization of the Foreign Intelligence Surveillance Act (FISA): Administration Proposes Broad Warrantless Surveillance of Citizens* (April 18, 2007).

[15] Foreign signals intelligence activities have many legitimate and necessary purposes beyond counterterrorism and counter-proliferation that need to be considered when crafting any framework that might inadvertently curtail these vital activities. It is beyond the scope of these comments, and, in any case, would be inappropriate in open session or public remarks, to discuss these additional requirements.

[16] Indeed, absent the FISA statute, there is no general warrant requirement for foreign intelligence surveillance under the Fourth Amendment. *See, e.g.*, United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980) (acknowledging the foreign intelligence exception to the Fourth Amendment warrant requirement), cert. denied, 454 U.S. 1144 (1982); *see also* United States v. United States District Court [Keith], 407 U.S.

Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence, 109th Congress, at 7-10 (Jul. 19, 2006) (Testimony of Kim Taipale, Center for Advanced Studies in Science and Technology Policy). [17]

Further, it is not clear in any case what substantive protections warrant procedures would add in this context—either they would prevent any signals intelligence activity from being used preemptively to identify threats (with devastating effect on the ability to gather foreign intelligence for any purpose), or they would become pro forma ministerial procedures with no substantive protections for privacy or civil liberties.

That the conventional law enforcement-derived warrant procedures might be an inappropriate method for authorizing legitimate foreign intelligence activities or might be ineffective to protect civil liberties when applied to certain kinds of intelligence activities is not a novel proposition. Testifying before the Church Committee in 1975, then-Attorney General Edward Levi suggested that FISA should explicitly include provisions for the approval of "programs of surveillance" in foreign intelligence situations where "by [their] nature [they do] not have specifically predetermined targets" and where "the efficiency of a warrant requirement would [therefore] be minimal." [18]

Programmatic approvals for certain foreign signals intelligence.

As noted above, the administration's proposals would exclude all non-targeted or non-domestic surveillance activity from FISA jurisdiction. While such an outcome would be in keeping with the intent of FISA as enacted, for the reasons discussed above, we think it would be useful for both Congress and the administration to consider whether a statutory mechanism for programmatic approval of certain foreign signals intelligence activity where there is a substantial likelihood of acquiring U.S. persons international or domestic communications would be appropriate. Such a mechanism would provide additional

---

297, 321-22 (1972) (warrant required for domestic security electronic surveillance, but Court explicitly disclaims any intent to decide whether warrant clause even applies to surveillance of foreign powers or their agents.). Further, there is no Fourth Amendment requirement for a warrant for incidental collection to a lawful intercept. Even under the stricter provisions governing ordinary criminal electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), *codified at* 18 U.S.C. §§ 2510-2521, incidental interception of a non-targeted person's conversations during an otherwise lawful surveillance would not be a violation of the Fourth Amendment. *See* United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985); *and* United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973).

[17] Available at http://intelligence.house.gov/Reports.aspx?Section=141. *See also The Ear of Dionysus, supra* note 7, at 134 n.16, 147 n.53, and158 n. 89.

[18] Likewise, even while requiring some form of judicial approval for *domestic* security surveillance, the court in Keith, *supra* note 16, suggested that different standards would be reasonable under the Fourth Amendment for security cases, noting that in such surveillance "the emphasis of ... intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency" and thus "the focus of ... surveillance may be less precise than that directed against more conventional types of crime" and that "exact targets of such surveillance may be more difficult to identify."

political, judicial, and public assurance that any foreign signals intelligence activity with a significant impact on domestic privacy or civil liberties was being lawfully conducted.

Programmatic approvals.

We have previously advocated that an explicit statutory mechanism be enacted, incorporating democratic checks-and-balances, for programmatic approval of certain foreign intelligence activities where there is a substantial likelihood of intercepting U.S. communications; in particularly, for those activities targeting specific foreign channels or targets, or using automated analysis or monitoring of foreign communication channels, where there is the likelihood of significant collateral intercepts of U.S. communications.

Various institutional mechanisms for programmatic approval and oversight of foreign intelligence surveillance programs have been suggested in connection with the NSA Terrorist Surveillance Program. These proposals have included executive, legislative, and judicial bodies. [19] Although I have briefly discussed the pros-and-cons of legislative versus judicial approvals on pages 10-12 of my HPSCI testimony, [20] I have not previously advocated any specific approval mechanism or standards. More recently, I have personally become persuaded by the arguments of John Schmidt, a former senior Justice Department official, that a statutory legal structure enacted by Congress authorizing direct judicial involvement in programmatic approvals would be most appropriate in order to foster the requisite political and public confidence in the legality of any authorized surveillance activities. [21]

The problem with the FISA procedures as currently constituted is that FISA provides only a single binary *a priori* threshold for authorizing any electronic interception—probable cause that the target is an agent of a foreign power. Unfortunately, even extensive contact with a known terrorist may not be procedurally sufficient to satisfy the current statutory requirements for a FISA warrant, and, more importantly, such contacts

---

[19] Compare, for example, Judge Richard Posner's proposal for an executive branch steering committee for national security electronic surveillance (*Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence*, 109th Congress (Jul. 19, 2006) (Testimony of Judge Richard A. Posner) at 4-5); the proposed Terrorist Surveillance Act of 2006, S.3931, 109th Congress (2006) (the DeWine bill) (oversight by special Congressional committees); the proposed National Security Surveillance Act of 2006, S.3876, 109th Congress (2006) (the Specter bill) (FISA court approval and oversight); John Schmidt, *Together Against Terror*, LEGALTIMES (Jan. 15, 2007) (FISC); and, the Electronic Surveillance Modernization Act, H.R. 5825, 109th Congress (2006) (the Wilson bill) (passed by the House on Sep. 28, 2006 and referred to the Senate Committee on the Judiciary) (requiring Congressional oversight but allow submission to the FISC for review).

[20] *See* note 17 *supra*.

[21] *See* John Schmidt, *Together Against Terror*, LEGALTIMES (Jan. 15, 2007); *The Ear of Dionysus*, *supra* note 7, at 156 n.84. Additional reporting and disclosure requirements, as well as enhanced oversight and review procedures should be considered as well.

Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence, 109th Congress, at 7-10 (Jul. 19, 2006) (Testimony of Kim Taipale, Center for Advanced Studies in Science and Technology Policy). [17]

Further, it is not clear in any case what substantive protections warrant procedures would add in this context—either they would prevent any signals intelligence activity from being used preemptively to identify threats (with devastating effect on the ability to gather foreign intelligence for any purpose), or they would become pro forma ministerial procedures with no substantive protections for privacy or civil liberties.

That the conventional law enforcement-derived warrant procedures might be an inappropriate method for authorizing legitimate foreign intelligence activities or might be ineffective to protect civil liberties when applied to certain kinds of intelligence activities is not a novel proposition. Testifying before the Church Committee in 1975, then-Attorney General Edward Levi suggested that FISA should explicitly include provisions for the approval of "programs of surveillance" in foreign intelligence situations where "by [their] nature [they do] not have specifically predetermined targets" and where "the efficiency of a warrant requirement would [therefore] be minimal." [18]

Programmatic approvals for certain foreign signals intelligence.

As noted above, the administration's proposals would exclude all non-targeted or non-domestic surveillance activity from FISA jurisdiction. While such an outcome would be in keeping with the intent of FISA as enacted, for the reasons discussed above, we think it would be useful for both Congress and the administration to consider whether a statutory mechanism for programmatic approval of certain foreign signals intelligence activity where there is a substantial likelihood of acquiring U.S. persons international or domestic communications would be appropriate. Such a mechanism would provide additional

---

297, 321-22 (1972) (warrant required for domestic security electronic surveillance, but Court explicitly disclaims any intent to decide whether warrant clause even applies to surveillance of foreign powers or their agents.). Further, there is no Fourth Amendment requirement for a warrant for incidental collection to a lawful intercept. Even under the stricter provisions governing ordinary criminal electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), *codified at* 18 U.S.C. §§ 2510-2521, incidental interception of a non-targeted person's conversations during an otherwise lawful surveillance would not be a violation of the Fourth Amendment. *See* United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985); *and* United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973).

[17] Available at http://intelligence.house.gov/Reports.aspx?Section=141. *See also The Ear of Dionysus, supra* note 7, at 134 n.16, 147 n.53, and158 n. 89.

[18] Likewise, even while requiring some form of judicial approval for *domestic* security surveillance, the court in Keith, *supra* note 16, suggested that different standards would be reasonable under the Fourth Amendment for security cases, noting that in such surveillance "the emphasis of ... intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency" and thus "the focus of ... surveillance may be less precise than that directed against more conventional types of crime" and that "exact targets of such surveillance may be more difficult to identify."

may only be discoverable through non-targeted or foreign directed signals intelligence activities in the first place. [22]

The FISC Orders of January 10, 2007.

Details of the FISC orders issued January 10, 2007 (authorizing certain activities previously carried out pursuant to Presidential authority under the NSA Terrorist Surveillance Program) [23] have not been publicly disclosed and the Justice Department has indicated that it is not prepared to release the orders to the public. [24] Speculation about the nature of the FISC orders has included discussion of whether they take the form of "anticipatory warrants" that would authorize surveillance in the future if certain factual predicates were to occur (including, for example, a known terrorist communicating with a someone in the U.S.). [25]

The Department of Justice has specifically denied, however, that these orders are "programmatic" in nature thus it is unlikely that they provide sufficient solution to the entirety of the problem of reconciling foreign signals intelligence activities with targeted domestic surveillance as discussed in these comments. Therefore, we still advocate a specific statutory basis for broader FISC jurisdiction and specific authority for "programmatic" approvals. Nevertheless, at the very least, it seems appropriate that an explicit statutory basis to support the January 10, 2007 FISC orders should be enacted.

Attorney General Levi foreshadowed an outcome in which anticipatory or programmatic warrants might be the appropriate mechanism to manage certain foreign signals intelligence activities when he suggested in his testimony to the Church Committee that a different kind of warrant based on submitting programs of surveillance (designed to gather foreign intelligence information essential to the security of the nation but not based on individualized suspicion) for judicial review might be developed. Here he cited Justice Powell's opinion in Almeida-Sanchez v. United States, 413 U.S. 266 (1973), in which the possibility of using "area warrants" to obtain "advance judicial approval of the decision to conduct roving searches on a particular road or roads for a reasonable period of time" was suggested approvingly. Levi went on to suggest that the development of any such new kind of extended warrant would benefit from an explicit statutory basis.

---

[22] For example, unlike with previous threats from other nation states or from ordinary crime, there may be no independent way to establish a connection to a foreign terrorist or proliferation group without the use of signals intelligence, particularly in cases where the recruitment and all contacts is conducted solely by electronic communications, for example, over the Internet.

[23] Letter from Alberto Gonzales, Attorney General of the United States, to Patrick Leahy, Chairman, and Arlen Specter, Ranking Member, Committee on the Judiciary, United States Senate (Jan. 17, 2007), *available at* http://fas.org/irp///agency/doj/fisa/ag011707.pdf.

[24] *See* Government's Supplemental Submission Discussing the Implications of the Intervening FISA Court Orders of Jan. 10, 2007 at 8-15, *ACLU v. NSA* (No. 06-CV-10204) (submission filed Jan. 24, 2007).

[25] The use of anticipatory warrants was upheld in U.S. v. Grubbs, 126 S. Ct. 1494, 1500 (2006) (warrant containing "triggering conditions" is constitutional).

He also suggested, however, that in dealing with foreign intelligence surveillance "it may be mistaken to focus on the warrant requirement alone to the exclusion of other, possibly more realistic, protections." Thus, programmatic approvals through statutory administrative or congressional authority should also be considered.

Non-content transactional data.

Although FISA currently has provisions for authorizing the targeted collection of non-content information—the FISA pen register and trap-and-trace provisions—it does not provide any procedures for authorizing even specific but non-targeted traffic or link analysis that may be required—and wholly reasonable—in the context of foreign signals intelligence to identify certain connections or threats.

For example, known patterns of terrorist communications can be identified and used to uncover other unknown but indirectly related terrorists or terrorist activity. Thus, for instance, in the immediate aftermath of 9/11 the FBI determined that the leaders of the 19 hijackers had made 206 international telephone calls to specific locations in Saudi Arabia, Syria, and Germany. It is believed that in order to determine whether any other unknown persons—so-called sleeper cells—in the United States might have been in communication with the same pattern of foreign correspondents the NSA analyzed Call Data Records (CDRs) of international and domestic phone calls obtained from the major U.S. telecommunication companies.

Undertaking such an analysis seems reasonable, particularly in the circumstances immediately following 9/11, yet FISA and existing procedures do not provide *any* approval or review mechanism for determining such reasonableness or for authorizing or governing such activity because FISA simply did not contemplate the current need for approval of specific—but non-targeted—pattern-based data searches or surveillance. [26]

Further, while it is well settled law that dialing or signaling information is entitled to lesser constitutional protection from disclosure than is content, [27] FISA as currently enacted is somewhat confusingly inconsistent about how such information is to be treated even in cases of targeted acquisition. FISA currently defines "content" to include "the identity of the parties to such communication or the existence" of the communication (*i.e.,* transactional information) but it also authorizes orders for pen registers and trap-and-trace devices to collect such information under a lesser standard than the statute requires for "content" intercepts.

---

[26] It is important to point out that the kind of automated traffic or link analysis being discussed here is not the undirected "data mining" to look for general indicia of "suspicious behavior" that rightly has civil libertarians concerned about fishing expeditions or general searches to examine all communication flows in the manner of a general warrant. See *The Ear of Dionysus, supra* note 7, at 150-156, 154 n.77. For a detailed discussion of general issues related to data mining, see the references in note 70, *id.* at 152.

[27] Smith v. Maryland, 442 U.S. 735 (1979).

The administration's FISA modernization proposals would address both the failure to anticipate the need for non-targeted traffic analysis and the inconsistency in statutory language for targeted collection by changing the definition of content to exclude transaction data and by simplifying the definition of "electronic surveillance" to only cover content interception. [28]

Again, while there is a strong case that the administration proposal is consistent with existing law and the original intent of FISA, nevertheless—for the same reasons set forth above regarding programmatic approval of content based signals intelligence—some statutory procedure to authorize and approve directed traffic or link analysis of transactional communication records where there is a significant impact on U.S. persons or domestic communications seems desirable as a matter of public policy.

The same kind of approval mechanisms discussed above for programmatic approvals might be applicable in these circumstances as well, recognizing, of course, that approvals for these activities should be subject to a lesser standard than those involving content, consistent with existing law.

Conclusion: FISA must be updated.

FISA as currently enacted fails to adequately enable legitimate and necessary foreign intelligence surveillance activity or to adequately protect privacy and civil liberties.

The administration is seeking to explicitly exclude from FISA statutory requirements those non-targeted or foreign signals intelligence activities that were not originally intended to be included in the FISA regime and that don't fit easily within its existing framework. Although we agree that this proposal is wholly consistent with the original intent of FISA, we are concerned that these kinds of activities increasingly impact the same domestic privacy and civil liberties interests that the political compromise leading to FISA was intended to address.

On the other hand, the critics of the administration's proposals are arguing simply to extend ill-suited FISA warrant procedures over activities that have different requirements and considerations than those for which FISA was designed and enacted. Force fitting these existing procedures to cover all signals intelligence activities that may affect U.S. persons is simply unworkable, is not constitutionally required, and would severely frustrate the ability to gather foreign intelligence information vital to the national security and interests of the United States.

The Center for Advanced Studies urges Congress to consider an adaptive legislative framework that will enable legitimate foreign intelligence activities while still protecting privacy and civil liberties; and that explicitly recognizes the different requirements and circumstances of signals intelligence and targeted wiretaps.

---

[28] Targeted collection of transactional information would still be subject to the pen register and trap-and-trace provisions of FISA,

We urge Congress to consider enacting an institutional mechanism for the programmatic approval, oversight, and review of legitimate foreign signals intelligence activity or programs where such activity is likely to have substantial impact on domestic privacy or civil liberties interests, as well as to provide some explicit guidelines governing how information derived from such programs can be reasonably used to protect the national security of the United States while still protecting privacy and civil liberties consistent with existing laws.

FISA as currently constituted is viable only for monitoring the activities of known agents of a foreign power but it is wholly ineffective for enabling or constraining the use of foreign signals intelligence to help identify threats in the first place or otherwise gather signals with foreign intelligence value to the United States. FISA must be updated to address these failures in order to protect both national security and individual freedom. Both values are indispensable and must be reconciled.

May 1, 2007.

THE EAR OF DIONYSUS: RETHINKING FOREIGN INTELLIGENCE SURVEILLANCE

K. A. TAIPALE*

9 YALE J. L. & TECH. 128 (2007)

TABLE OF CONTENTS

TABLE OF CONTENTS .....
INTRODUCTION .....
I. FOREIGN INTELLIGENCE SURVEILLANCE: A BRIEF OVERVIEW .....
II. CHANGING BASE CONDITIONS .....
A. THE CHANGING NATURE OF THE THREAT AND THE SHIFT TO PREEMPTION .....
B. THE NEED FOR SURVEILLANCE .....
C. THE DISSOLVING PERIMETER OF DEFENSE .....
III. THE EAR OF DIONYSUS .....
A. FISA IS INADEQUATE .....
B. TRANSIT INTERCEPTS: FROM CIRCUIT-BASED TO PACKET-BASED COMMUNICATION NETWORKS .....
C. COLLATERAL INTERCEPTS: THE GLOBALIZATION OF COMMUNICATIONS .....
D. AUTOMATED ANALYSIS: CONTENT FILTERING, TRAFFIC ANALYSIS, AND LINK OR PATTERN ANALYSIS .....
IV. FIXING FOREIGN INTELLIGENCE SURVEILLANCE .....
CONCLUSION .....

A précis of this article was published as *Rethinking Foreign Intelligence Surveillance*, WORLD POLICY J. (Vol. XIII No. 4, Winter 2006-2007), *available at* http://www.mitpressjournals.org/doi/pdf/10.1162/wopj.2007.23.4.77.

* *Kim Taipale is the founder and executive director of the Center for Advanced Studies in Science and Technology Policy. He is also a senior fellow at the World Policy Institute, a member of the Markle Task Force on National Security in the Information Age, and an adjunct professor of law at New York Law School. His other writings can be found online at http://taipale.info/.*

INTRODUCTION

As the 110th Congress begins to flex its atrophied oversight muscle,[1] it bears remembering that, in the ongoing debate over *who* should have the authority to authorize and oversee foreign intelligence surveillance programs,[2] *someone* must,[3] and the existing mechanisms, in particular, the Foreign Intelligence Surveillance Act of 1978 ("FISA")[4] and its related

---

[1] *See, e.g.*, Donna Leinwand, *Senators Press Gonzales on Delay in Getting Court Okay on Surveillance*, USA TODAY, Jan 19, 2007, at 4A; Lara Jakes Jordan, *Senators Grill Gonzales Over Spy Program*, SUN-SENTINEL (Fort Lauderdale, Fla.), Jan. 19, 2007, at 6A; Tom Brune, *Surveillance Questioned: Gonzales, Senate Judiciary Committee Battle Over Decision by Special Courts*, NEWSDAY, Jan. 18, 2007, at A26; *and* Jeff Bliss, *Rockefeller Says He May Subpoena Documents on Spying*, BLOOMBERG NEWS, Jan. 26, 2007. *See generally* Brian Knowlton, *Top Democrat seeks wider NSA hearings*, INT'L HERALD TRIB., Jan. 1, 2006, *available at* http://www.iht.com/articles/2006/01/01/news/policy.php; Shaun Waterman, *Dems Take Over Hill Intel Panels*, UPI, Dec. 8, 2006 ("Democrats say . . . they will launch a vigorous push for oversight of some of the most secret and controversial programs . . . employed in the war on terror . . . ."); *and* Eric Lichtblau, *With Power Set to Be Split, Wiretaps Re-emerge as Issue*, N.Y. TIMES, Nov. 10, 2006, at A28 ("Democrats . . . vowed to investigate the [National Security Agency Terrorist Surveillance Program] aggressively once they assume power").

[2] This public debate has taken place within the context of media disclosures regarding certain classified operational programs of the National Security Agency ("NSA"), including the Terrorist Surveillance Program ("TSP") in which certain international calls of suspected terrorists were being monitored pursuant to presidential authority without warrants in circumstances that otherwise might implicate the warrant requirements of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), *see* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, and an alleged program to collect and analyze Call Detail Records (CDRs) from U.S. telecommunication carriers, *see* Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY, May 11, 2006), at A1. On January 17, 2007, Attorney General Alberto Gonzales informed the chairman and ranking member of the U.S. Senate Committee on the Judiciary by letter that the Foreign Intelligence Surveillance Court ("FISC") had issued orders on January 10, 2007 authorizing certain surveillance previously authorized under the NSA TSP (the "FISC orders"). The letter stated that as a result of these orders, "any electronic surveillance that was [previously] occurring as part of the [TSP] will now be conducted subject to the approval of the [FISC]" and, accordingly, that "the President has determined not to reauthorize the [program] when the current authorization expires." For the reasons outlined in this article, FISA should be amended to provide an explicit statutory basis for these orders to address the problems outlined herein. Letter from Alberto Gonzales, Attorney General of the United States, to Patrick Leahy, Chairman, and Arlen Specter, Ranking Member, Committee on the Judiciary, United States Senate (Jan. 17, 2007), *available at* http://fas.org/irp///agency/doj/fisa/ag011707.pdf.

[3] *See* Knowlton, *supra* note 1 ("[Senator] Schumer [D-NY] said the problem was not with good-faith efforts to make Americans secure—no Democrat opposed that, he said—but with the president's authority to do so unilaterally.").

[4] Pub. L. No. 95-511, Title I, 92 STAT. 1783 (1978) (codified as amended at 50 U.S.C. §§ 1801-11, 1821-29, 1841-46, & 1861-62). FISA provides a framework for using electronic surveillance, physical searches, pen registers and trap and trace devices to acquire "foreign intelligence information."

procedures, are no longer adequate and must be updated. The FISA simply did not anticipate the nature of the current threat to national security from transnational terrorism, nor did it anticipate the development of global communication networks or advanced technical methods for intelligence gathering.

New technologies do not determine human fates, but they do alter the spectrum of potentialities within which people act.[5] This article examines how technology and certain related developments have enabled new threats and new response mechanisms that challenge existing policy constructs and legal procedures in the context of foreign intelligence surveillance.[6] This article does not argue that these developments justify abandoning long-held bedrock principles of democratic liberty—nor even that some new "balance" between security and liberty need be achieved[7] — rather, it argues that familiar, existing oversight and control mechanisms—including FISA—or their analogues can be applied in these novel, technologically-enabled circumstances, but only if the challenges and opportunities are better understood and the laws and procedures updated to accommodate needed change.

This article is intended neither as critique nor endorsement of any particular government surveillance program or action;[8] rather, it attempts to

---

[5] ROBERT MCCLINTOCK & K. A. TAIPALE, INSTITUTE FOR LEARNING TECHNOLOGIES AT COLUMBIA UNIVERSITY, EDUCATING AMERICA FOR THE 21ST CENTURY 2 (1994).

[6] It is beyond the scope of this article to address how these developments affect other national security and law enforcement policy, or to address the underlying philosophical or political issues regarding appropriate social-control mechanisms more generally. However, these developments take place within an ongoing transformation of modern societies from a notional Beccarian model of criminal justice based on accountability for deviant actions after they occur, *see generally* CESARE BECCARIA, ON CRIMES AND PUNISHMENT (1764), to a Foucauldian model based on authorization, preemption, and general social compliance through ubiquitous preventative surveillance and control through system constraints. *See generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH (Alan Sheridan trans., 1977). In this emergent model, 'security' is geared not towards traditional policing through arrest and prosecution but to risk management through surveillance, exchange of information, auditing, communication, and classification. *See generally* THE NEW POLITICS OF SURVEILLANCE AND VISIBILITY (Kevin D. Haggarty & Richard V. Ericson eds., 2006) (discussing the collection and analysis of information for social-control).

[7] Indeed, I have argued elsewhere that the very notion of balance is misleading and deflects the discourse since implicit in the use of balance as metaphor is that some fulcrum point exists at which the correct amount of security and liberty can be achieved. However, liberty and security are not dichotomous rivals to be traded one for the other in some zero sum game but rather each vital interests to be reconciled, and, thus, dual obligations to be met. *See, e.g.*, K. A. Taipale, *Introduction to Domestic Security and Civil Liberties*, *in* THE MCGRAW-HILL HOMELAND SECURITY HANDBOOK 1009-12 (David Kamien ed., 2006); *and* K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy, and the Lessons of King Ludd*, 7 YALE J. L. & TECH. 123, 126-8 (2004) (hereinafter, "*Frankenstein*").

[8] In particular, neither of the classified programs referred to in note 2, *supra*; however, certain aspects of the TSP are discussed in general terms in Section III, *infra*.

highlight certain issues critical to a reasoned debate and democratic resolution of these issues. Further, this article does not address directly whether the President currently has inherent or statutory authority to approve any specific operational program[9] nor whether press disclosure of classified government programs is appropriate or justified.[10]

---

[9] Whether the President has inherent or statutory authority to authorize foreign intelligence surveillance programs, including the TSP, is currently being litigated. *See* ACLU v. NSA, No. 06-CV-10204 (E.D. Mich., filed Jan. 17, 2006); and Center for Constitutional Rights v. Bush, No. 06-CV-00313 (S.D.N.Y., filed Jan. 17, 2006); *and* Hepting v. AT&T No. C-06-0672-JCS (N.D. Ca., filed Jan. 31, 2006) (class action suit against AT&T and other telecommunications providers for participating in the NSA surveillance programs).

On Aug. 17, 2006, the district court in ACLU v. NSA ruled that the TSP was illegal under FISA and unconstitutional under the First and Fourth Amendments. That opinion has been heavily criticized. *See, e.g.*, Jack Balkin, *Federal court strikes down NSA domestic surveillance program*, Balkinization (Aug. 17, 2006), *available at* http://balkin.blogspot.com/2006/08/federal-court-strikes-down-nsa.html ("much of the opinion is disappointing, and . . . a bit confused"); *and* Editorial, *A Judicial Misfire*, WASH. POST, Aug. 18, 2006, at A20 (The decision "is neither careful nor scholarly" and "as a piece of judicial work—that is, as a guide to what the law requires and how it either restrains or permits the NSA's program—[the] opinion will not be helpful"). On Oct. 4, 2006, a unanimous three-judge panel of the United States Court of Appeals for the Sixth Circuit stayed the district court's ruling while the government's appeal is considered. On Jan. 24, 2007, the Justice Department asked that the case be dismissed as moot. *See* Dan Eggen, *Dismissal of Lawsuit Against Warrantless Wiretaps Sought*, WASH. POST, Jan. 26, 2007, at A5 ("A lawsuit challenging the legality of the National Security Agency's warrantless surveillance program should be thrown out because the government is now conducting the wiretaps under the authority of a secret intelligence court, according to court papers filed by the Justice Department yesterday"). *See* Government's Supplemental Submission Discussing the Implications of the Intervening FISA Court Orders of Jan. 10, 2007 at 8-15, ACLU v. NSA, No. 06-CV-10204, (submission filed Jan. 24, 2007). On Jan. 31, 2007, a three-judge panel of the Sixth Circuit Court of Appeals heard oral arguments on these issues. *See* Adam Liptak, *Judges Weigh Arguments In U.S. Eavesdropping Case*, N.Y. TIMES, Feb. 1, 2007, at A12.

Testifying in 1976 that the President must retain some Constitutional power to conduct surveillance beyond FISA despite the "exclusivity" provision set forth in 18 U.S.C. § 2511(2)(f) ("...procedures in ... the [FISA] shall be the exclusive means by which [foreign intelligence] electronic surveillance ... may be conducted"), President Gerald Ford's Attorney General Edward Levi asserted that there is "a presidential [surveillance] power which cannot be limited, no matter what Congress says." Levi, a well-respected constitutional scholar and formerly the dean of the University of Chicago Law School, testified that "[t]he very nature of the reserved presidential power, the reason it is so important, is that some kind of emergency could arise which I cannot foresee now, nor, with due deference to Congress, do I believe Congress can foresee." *Foreign Intelligence Surveillance Act of 1976, Hearing on S. 743, S. 1888 and S. 3197, before the Subcommittee on Criminal Laws and Procedures of the Committee on the Judiciary United States Senate*, 94th Cong., 17-18 (1976) (testimony of Edward H. Levi, Attorney General) quoted in John Schmidt, *When Terrorists Talk...* , LEGALTIMES, Sep. 18, 2006 (discussing the exclusivity provision of FISA and the President's inherent surveillance power). In particular, Levi warned "that the unpredictability of foreign threats to the nation and *the likelihood of ongoing changes in communication technologies* made it 'extraordinarily dangerous' to ...

This article is organized into six parts: this *Introduction*, four descriptive sections, and a brief *Conclusion*. *Section I: Foreign Intelligence Surveillance: A Brief Overview* provides a very brief introduction to the relevant parts of the FISA regime; *Section II: Changing Base Conditions* describes the changing nature of the threat, the shift to preemptive strategies in response, and the need for surveillance to support preemption; *Section III: The Ear of Dionysus* describes the nature of modern communication networks and certain related technology developments, and examines how three situations—*transit intercepts*, *collateral intercepts*, and *automated monitoring*—cannot be accommodated by FISA as currently constituted (this section also briefly speculates on certain aspects of the TSP); and, *Section IV: Fixing Foreign Intelligence Surveillance* suggests some potential solutions that preserve existing Fourth Amendment principles and protections while still addressing these failures. Finally, the *Conclusion*

---

not acknowledge the president's retained surveillance power" *Id.* (emphasis added). While I take no position in this article on whether, indeed, the President retains inherent surveillance powers, I do believe that the issues discussed herein are among those kinds of unforeseen circumstances that Levi foreshadowed.

[10] For example, on June 23, 2006, *The New York Times* disclosed another secret program that allegedly "trac[ed] transactions of people suspected of having ties to Al Qaeda by reviewing records [of wire transfers] from [the Society for Worldwide Interbank Financial Telecommunication ("Swift")] ... a Belgian cooperative that routes about $6 trillion daily between banks, brokerages, stock exchanges and other institutions." Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, Jun. 23, 2006, at A1. Subsequently, *The New York Times* Public Editor Byron Calame published a *mea culpa* in which he wrote "I don't think the [Swift] article should have been published" because the program was clearly legal under U.S. law and there were no allegations that any information had been misused. Byron Calame, *Banking data: A Mea Culpa*, N.Y. TIMES, Oct. 22, 2006, at A12. However, according to then House Intelligence Committee Chairman Pete Hoekstra (R-MI), "The mea culpa of the *New York Times* public editor comes too late to stop the damage done to one of our nation's leading tools to track, understand and prevent the money transfers that enable terrorist attacks." Press Release, Hoekstra Statement on New York Times Mea Culpa, Oct. 25, 2006, *available at* http://hoekstra.house.gov/News/DocumentSingle.aspx?DocumentID=51935; *see also* Editorial, *Not So Swift*, WASH. TIMES, Oct. 24, 2006, at A16 ("The [N.Y.] Times never adequately defended its exposure of the program ... if no illegality or immoral action has taken place, and there is a very high risk of genuinely endangering national security, the decision must be against publication ... sometimes the media simply needs to let government do its job").

For consideration of whether *The New York Times* violated the Espionage Act, 18 U.S.C. § 798 (2000) (Disclosure of classified information), when it disclosed the TSP, *see* Gabriel Schoenfeld, *Has the "New York Times" Violated the Espionage Act?* COMMENTARY, March 2006, at 23 ("The real question ... is whether ... we as a nation can afford to permit the reporters and editors of [the *New York Times*] to become the unelected authority that determines for all of us what is a legitimate secret and what is not. ... The laws governing [the disclosure of the TSP by the *Times*] are perfectly clear, will they be enforced?" *Id.* at 31). *See also Digital Age with James C. Goodale: "Will Bush Indict The New York Times?"* (WNYE-PBS television broadcast, Mar. 4, 2007).

reiterates the need to get beyond backward looking recriminations and to craft progressive consensual solutions.

I. FOREIGN INTELLIGENCE SURVEILLANCE: A BRIEF OVERVIEW

Of relevance to the discussion in this Article,[11] FISA generally prescribes procedures requiring a court order for conducting electronic surveillance to gather "foreign intelligence information"[12] when such surveillance targets United States persons[13] or is conducted within the United States.[14] FISA was never intended to apply to wholly foreign communications of non-U.S. persons nor to be triggered by incidental interceptions of U.S. person communications during legitimate foreign intelligence intercepts not themselves subject to FISA.[15] However, as

---

[11] This article concerns itself with certain specific aspects of electronic surveillance—in particular the interception of 'signals of interest' in packet-based communication networks—and the related technology and policy developments. Thus, it is beyond the scope of this article to fully delineate FISA and the related foreign intelligence surveillance law. For a detailed discussion of FISA, *see* ELIZABETH B. BAZEN, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND RECENT JUDICIAL DECISIONS, (Congressional Research Service Report for Congress No. RL30465, 2007).

[12] "Foreign intelligence information" is information that "relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power or (B) international terrorism by a foreign power or an agent of a foreign power . . . ." 50 U.S.C. § 1801(e) (2000).

[13] "United States person" means a U.S. citizen or lawfully resident alien. 50 U.S.C. § 1801(i) (2000).

[14] "Electronic surveillance" means—

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, ... ;
>
> ...

50 U.S.C. § 1801(f) (2000)

[15] Communications of a U.S. person acquired during or incidental to a lawful foreign collection would generally be subject to minimization procedures consistent with Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted as amended in* 50 U.S.C. § 401 note, and related guideline documents. Part 2.3 (c) of the executive order would permit retention and dissemination of "information obtained in the course of a lawful ... international terrorism investigation" subject only to normal minimization requirements. *See* note 54 *infra* and accompanying text. *Cf.* note 91 *infra* (discussing restrictions in practice that prevent

discussed in Section III below, technical developments unanticipated by FISA are triggering warrant requirements in circumstances that were not contemplated or intended when FISA was enacted.[16]

Further, FISA is intended to provide a statutory mechanism to authorize electronic surveillance of U.S. persons or within the U.S. when there is probable cause to believe the target is an "agent of a foreign

---

effective use in certain circumstances of incidental intercepts of U.S. person communications). Executive Order 12,333 allows the collection, retention, or dissemination of information about U.S. persons pursuant to procedures established by the head of each intelligence agency and approved by the Attorney General.

> The [Central Intelligence Agency] procedures are embodied in Headquarters Regulation (H.R.) 7-1 entitled, "Law and Policy Governing the Conduct of Intelligence Activities." NSA is governed by Department of Defense Directive 5240.1-R, "DoD Activities that May Affect U.S. Persons," including a classified appendix particularized for NSA [*see* partially declassified *Annex – Classified Annex to DoD Procedures under Executive Order 12,333* to NSA/CSS POLICY 1-23 (Mar. 11, 2004)]. The guidelines are further enunciated within NSA through an internal directive, [NSA/Central Security Services] U.S. Signals Intelligence Directive 18 [Jul. 27, 1993, hereinafter "USSID 18"]. The FBI procedures are contained in "Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations" [Mar. 1999] [these guidelines were updated and revised in *Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (effective Oct. 31, 2003)].

NATIONAL SECURITY AGENCY, REPORT TO CONGRESS: LEGAL STANDARDS FOR THE INTELLIGENCE COMMUNITY IN CONDUCTING ELECTRONIC SURVEILLANCE (2000), *available at* http://www.fas.org/irp/nsa/standards.html.

[16] For example, when wholly foreign communications are targeted from a telecommunications switch in the United States and a communication "to or from the U.S." is incidentally intercepted, thus, implicating 50 U.S.C. § 1801(f)(2), see the discussion of transit and collateral intercepts in Section III, *infra*. *And see* notes 41 and 49 *infra*. Note that any implied warrant requirement in these circumstances is only a statutory requirement as there is no general Fourth Amendment requirement for a warrant for incidental collection from a lawful intercept. Even under the stricter provisions governing ordinary criminal electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968), *codified at* 18 U.S.C. §§ 2510-2521, incidental interception of a non-targeted person's conversations during an otherwise lawful surveillance would not be a violation of the Fourth Amendment. *See* United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985); *and* United States v. Tortorello, 480 F.2d 764 (2d Cir. 1973). Indeed, absent the FISA statute, there may be no general Fourth Amendment warrant requirement for any foreign intelligence surveillance. *See, e.g.*, United States v. Truong, 629 F.2d 908, 914 (4th Cir. 1980) (acknowledging the foreign intelligence exception to the Fourth Amendment warrant requirement); *see also* United States v. United States District Court [Keith], 407 U.S. 297, 321-22 (1972) (warrant required for domestic security electronic surveillance, but Court explicitly disclaims any intent to decide whether warrant clause applies to surveillance of foreign powers or their agents).

power,"[17] thus, is useful for monitoring known agents of an enemy power. FISA did attempt to address the then nascent threat of international terrorism by defining "foreign power" to include "a group engaged in international terrorism or activities in preparation therefore" for purposes of the statute.[18] However, for reasons discussed in Section II, the nature of the current global terrorist threat does not easily conform to "agent of a foreign power" equivalence for these purposes.

Finally, FISA provides only a single cumbersome binary mechanism that requires an individual application to the Foreign Intelligence Surveillance Court ("FISC") for authorization to target a specific individual or communication to or from the United States based on an *pre hoc* showing of probable cause that the target is acting as an agent of a foreign power or foreign terrorist group,[19] but provides no mechanisms for authorizing

---

[17] 50 U.S.C. § 1805(a)(3)(A) (2000).

[18] 50 U.S.C. § 1801(a)(4) (2000). However, the prevailing paradigm of 'international terrorism' at the time that FISA was enacted generally consisted of isolated attacks conducted abroad against U.S. national interests. *See also* note 34 *supra*.

The definition of "agent of a foreign power" was further stretched in 2003 to include so-called "lone wolves." §1801(b)(1)(C). (The 'lone wolf' amendment is often referred to as the "Moussaoui fix." *See, e.g.*, Press Release, Office of Senator Charles E. Schumer, Schumer, Kyl to Introduce Moussaoui-fix, Jun. 5, 2002, *available at* http://www.senate.gov/~schumer/SchumerWebsite/pressroom/press_releases/PR01025.html.

[19] In the case of a U.S. person, FISA requires probable cause to believe that the target is an "agent of a foreign power," 50 U.S.C. § 1801(b) and that the person's activities "involve or are about to involve" a violation of the criminal laws of the United States, § 1801(b)(2)(B); or are activities in preparation for sabotage or "international terrorism" on behalf of a foreign power, § 1801(b)(2)(C).

A court order authorizing electronic surveillance to target a specific person or communication for foreign intelligence purposes is sought under 50 U.S.C. § 1804 by application of a federal officer in writing on oath or affirmation to a FISC judge after approval by the Attorney General based upon his finding that the criteria and requirements set forth in 50 U.S.C. § 1801 *et seq.* have been met. Section 1804(a) sets out specifically what must be included in the application and § 1805(a) sets out the findings and probable cause standards required of the FISC judge. Finally, § 1805(c) sets out the limitations that must be specified in the order.

In addition to the inflexibility of the FISA warrant procedures to accommodate the circumstances described later in this article, the efficacy of requiring traditional warrants in all cases for foreign intelligence surveillance was itself questioned by then Attorney General Edward Levi in 1975:

> Levi said ... [f]oreign intelligence ... may in some situations require "virtually continuous surveillance, which by its nature does not have specifically predetermined targets." In these situations, "the efficiency of a warrant requirement would be minimal."

John Schmidt, *A Historical Solution to the Bush Spying Issue*, CHIC. TRIB., Feb. 12, 2006. *See also Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence*, 109th Cong. (2006) (testimony of Judge Richard A. Posner) (questioning the relevance of the warrant requirement to certain aspects of foreign intelligence surveillance).

advanced technical methods (including those discussed in this article) to help identify such agents in the first place.

II. CHANGING BASE CONDITIONS

Both security and liberty today function within a changing technological context, but mere recognition of changed circumstance itself is not sufficiently determinative of desirable outcomes. It is acceptable neither to say that 'everything changed on 9/11' and thus we must accept lessened liberty, nor to say that we have 'faced greater threats before' and thus we should cling to outmoded praxis developed at another time, to deal with a different threat.[20] Rather, changing context requires reflective reexamination of previously satisfactory practices based on an informed appreciation of the complex interactions of new threats with new opportunities, and with a willingness to reconstruct outmoded habitudes. While we cannot simply abandon cherished values because maintaining them is difficult, neither can we simply resist change because it is uncomforting.

A. THE CHANGING NATURE OF THE THREAT AND THE SHIFT TO PREEMPTION

Enabled in part by force-multiplying technologies, the potential to initiate catastrophic outcomes to national security is devolving from other nation states (the traditional target of national security power) to organized

[20] Thus, it is particularly delusive to believe that because we successfully faced a greater destructive threat from the Soviet Union that we can also successfully meet the current threat with the same outdated strategies or tools, that is, without adapting to change. It is the qualitative nature of the current threat, not just its quantitative force that needs to be considered in devising successful counterstrategies. For example, accountability strategies useful for countering nation state adversaries—for example, pursuing nuclear deterrence through a doctrine of mutual assured destruction (MAD)—must be recognized as ineffective against attackers unconstrained by after-the-fact punishment, in particular, suicide attackers without accountable patrons or other support infrastructure subject to sanction or retaliation. Even previously successful counterinsurgency strategies—for example, providing participatory political opportunities—will likely be ineffective against an enemy inherently opposed to rule through democratic structures. So, too, law enforcement strategies developed to deal with organized crime or other economically motivated conspiracies like drug smuggling are inadequate when employed against ideologically motivated forces. For a discussion of strategic counterterrorism options, see generally BARD E. O'NEILL, INSURGENCY AND TERRORISM (2d. ed., rev'd, 2005); DANIEL BENJAMIN & STEVEN SIMON, THE NEXT ATTACK: THE FAILURE OF THE WAR ON TERROR AND A STRATEGY FOR GETTING IT RIGHT (2005). For a discussion of defensive strategies for homeland security, see generally MICHAEL D'ARCY, *ET AL.*, PROTECTING THE HOMELAND 2006/2007 (2006). For a discussion of the role of the U.S. intelligence system in counterterrorism, see generally RICHARD A. POSNER, UNCERTAIN SHIELD: THE U.S. INTELLIGENCE SYSTEM IN THE THROES OF REFORM (2006).

but stateless groups (the traditional target of law enforcement power) blurring the previously clear demarcation between reactive law enforcement policies and preemptive national security strategies.[21] Organized groups of non-state actors now have the potential capacity[22] and capability[23] to inflict the kind of destructive outcomes that can threaten national survival by undermining the public confidence that maintains the economic and political systems in modern Western democracies.[24] In simple terms, the threat to national security is no longer confined only to other nation states.[25]

---

[21] *See generally* Taipale, *Frankenstein*, *supra* note 7 at 129-35; and K. A. Taipale, *Designing Technical Systems to Support Policy: Enterprise Architecture, Policy Appliances, and Civil Liberties*, *in* EMERGENT INFORMATION TECHNOLOGIES AND ENABLING POLICIES FOR COUNTER TERRORISM 442-43 (Robert Popp & John Yen eds., Jun. 2006).

[22] Technologically-enabled capacities include the use of so-called weapons of mass destruction (WMDs), including chemical, biological, and nuclear (CBN) weapons, the use of airliners or other advanced technology infrastructure as a weapon system, or the targeting of technological vulnerabilities, for example, critical infrastructure control systems (in particular, Supervisory Control and Data Acquisition systems or SCADA). *See, e.g.*, Alan Joch, *Terrorists Brandish Tech Sword, Too*, FEDERAL COMPUTER WEEK, Aug. 28, 2006.

[23] Technologically-enabled capabilities include world-wide recruitment, organization, funding, planning, training, targeting, and command-and-control using global communication networks and the Internet. *See, e.g.*, Joch, *supra* note 22. In addition, these developments allow direct access to, or circumvention of, mainstream information distribution channels for propaganda purposes. For an overview of terrorist use of the Internet, see generally GABRIEL WEIMANN, TERROR ON THE INTERNET: THE NEW ARENA, THE NEW CHALLENGES (2006) (see, in particular, the discussion of communicative uses of the Internet at 49-110; and instrumental uses at 111-46).

[24] In addition to the approximately 3,000 immediate deaths resulting from the terrorist attack on the World Trade Center and Pentagon, the attack has been variously estimated to have caused between $50 billion and $100 billion in direct economic loss. Estimates of indirect losses in the immediate aftermath exceeded $500 billion nationwide. GENERAL ACCOUNTING OFFICE, U.S. CONGRESS, GAO-02-700R, REVIEW OF STUDIES OF THE ECONOMIC IMPACT OF THE SEPTEMBER 11, 2001 TERRORIST ATTACKS ON THE WORLD TRADE CENTER (2002). In the eighteen months following the attacks, 2.5 million jobs were estimated to have been lost in the United States. Brian Sullivan, *Job Losses Since 9/11 Attacks Top 2.5 Million*, COMPUTERWORLD, Mar. 25, 2003. The total cost of knock-on effects, including the cost to national economic efficiency, competitiveness, and civil liberties from policies implemented in the response to the attacks are incalculable.

[25] Indeed, technology is affording non-state competitors—including international terrorist groups, organized crime gangs, rogue multinational corporations, and other hostile NGOs—the potential to exercise economic, political, and military power, including violence, at a scale that has traditionally been subject to sovereign nation state monopoly and which is beyond the reach of any single nation state's jurisdiction to control, thus potentially undermining the entire Westphalian construct of international political relations. However, it is beyond the scope of this article to address these broader issues. *See generally* MARTIN VAN CREVELD, THE RISE AND DECLINE OF THE STATE 377-94 (1999) ("Technology Goes International").

As Thomas Friedman writes in *The World is Flat*, 21st Century terrorism is the globalization of 20th Century terrorism.[26]

Thus, there has emerged a political consensus, at least with regard to certain threats, to take a preemptive rather than reactive approach.[27] "Terrorism cannot be treated as a reactive law enforcement issue, in which we wait until after the bad guys pull the trigger before we stop them."[28] The policy debate, then, is not about preemption itself—even the most strident civil libertarians concede the need to identify and stop terrorists before they act[29]—but instead revolves around what methods are to be properly employed in this endeavor.

B. THE NEED FOR SURVEILLANCE

Preemption of terrorist attacks that can occur at any place and any time requires information useful to anticipate and counter future events—that is, it requires actionable intelligence.[30] Since terrorist attacks at scales

---

[26] THOMAS FRIEDMAN, THE WORLD IS FLAT (2006). Globalized transnational terrorism, enabled and empowered in part by technology developments, *see* notes 22 & 23 *supra*, is simply qualitatively different than the then nascent "international terrorism" threat that was belatedly addressed in FISA by simply expanding the definition of "foreign power" to include "group[s] engaged in international terrorism" 50 U.S.C. § 1801(a)(4) (2000); *see also* note 18 *supra* and note 34 *infra*. *See generally* NETWORKS, TERRORISM AND GLOBAL INSURGENCY (Robert J. Bunker ed., 2005) (assessing the threat posed by global terrorism).

[27] It is beyond the scope of this article to delineate precisely where the line should be drawn between threats requiring a preemptive approach and those that remain amenable to traditional reactive law enforcement. For purposes of this article, we assume that there is some threat from loosely organized global terrorist groups that implicates national security and therefore requires a preemptive approach. *See, e.g.*, Osama Bin Laden, *Declaration of War against Americans Occupying the Land of the Two Holy Places* (1996), *available at* http://www.pbs.org/newshour/terrorism/international/fatwa_1996.html; Osama Bin Laden, *et al.*, *Jihad Against the Jews and Crusaders*, World Islamic Front Statement (1998), *available at* http://www.fas.org/irp/world/para/docs/980223-fatwa.htm. However, it is not appropriate, nor realistic, to assume that all manner of 'terrorist' acts are subject to preemptive strategies or are preventable. It is axiomatic that national security assets, including foreign intelligence surveillance capabilities, should be employed only against true threats to national security and not used for general law enforcement or other social-control purposes.

[28] Editorial, *The Limits of Hindsight*, WALL ST. J., Jul. 28, 2003, at A10. *See also* U.S. DEPARTMENT OF JUSTICE, FACT SHEET: SHIFTING FROM PROSECUTION TO PREVENTION, REDESIGNING THE JUSTICE DEPARTMENT TO PREVENT FUTURE ACTS OF TERRORISM (2002).

[29] *See, e.g.*, *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before U.S. Senate Committee on the Judiciary*, 110th Cong. (2007) (statement of Sen. Edward Kennedy, Member, Comm. on the Judiciary) ("We all agree on the need for strong powers to investigate terrorism [and] prevent future attacks . . . .").

[30] Terrorism, by indiscriminately targeting civilians and infrastructure, limits the effectiveness of certain other counterstrategies that are otherwise useful, i.e., those useful against nation state adversaries conforming to the international laws of armed conflict

C. THE DISSOLVING PERIMETER OF DEFENSE

The final characteristic of the current terrorist threat to be considered in this section is that the perimeter of effective defense is dissolving. The traditional "line at the border" based defense, useful against threats from other nation states, is insufficient against a parlous enemy[35] that moves easily across borders and hides among the general population, taking advantage of open societies to mask its own organization and activities.[36] Thus, arbitrary national boundary-based rules for conducting electronic surveillance—like those in FISA that are triggered by activity "within the United States" or involving "U.S. persons"—that do not conform to actual patterns of global terrorist activity (and which may have been perfectly adequate in prior contexts with known or identifiable adversaries) are deficient to deal with ambiguous threats.

---

in international terrorism" as "foreign powers" for purposes of the statute, 50 U.S.C. § 1801(a)(4) (2006), it simply did not contemplate the nature or scale of a globalized, non-state group conspiracy enabled by modern technology that could directly attack the U.S. homeland or generally threaten long-term national security, nor did it anticipate the need to use advanced technical methods to help identify and preempt such threats.

For a brief overview of the nature of modern terrorism see WEIMANN, *supra* note 23 at 20-23. In particular, see the discussion contrasting an intentionally oversimplified dichotomy of "old" and "new" terrorism, *id.* at 22, for which Weimann cites Shabtai Shavit, *Contending with International Terrorism*, 6 J. INT'L SECURITY AFF. 63-75 (2004) (proposing a permanent international mechanism to combat terrorism. *Id.* at 73-75).

[35] *See* bin Laden, *supra* note 27, and World Islamic Front Statement, *supra* note 27. *See also* Nassir bin Hamd al-Fahd, *Risalah fi hokum istikhdam aslihat al-damar al-shamel didh al-kuffar* (May 2003) (fatwa on the permissibility of WMD in jihad) *cited in* Robert Wesley, *Al-Qaeda's WMD Strategy After the U.S. Intervention in Afghanistan*, TERRORISM MONITOR, Vol. 3 Iss. 20, Oct. 21, 2005; CHRISTOPHER M. BLANCHARD, AL QAEDA: STATEMENTS AND EVOLVING IDEOLOGY (Congressional Research Service Report to Congress No. RL32759, 2007); ANONYMOUS, THROUGH OUR ENEMIES EYES at xii (2002) ("The United States is embroiled in a momentous struggle . . . . bin Laden . . . and . . . the movement he established is a foe that must be understood before his movement can be, and must be, defeated and eliminated").

[36] Although there is an ongoing global conspiracy hostile to U.S. interests with an identifiable core, the threat has metastasized to more autonomous and decentralized organizational structures creating additional challenges for security services. *See, e.g.*, *The Changing Face of Terror: A Post 9/11 Assessment, Testimony Before the Senate Committee on Foreign Relations by Ambassador Henry A. Crumpton, Coordinator for Counter-terrorism*, (Jun. 13, 2006) *available at* http://www.senate.gov/~foreign/testimony/2006/CrumptonTestimony060613.pdf. *See generally* DANIEL BENJAMIN & STEVEN SIMON, THE NEXT ATTACK (2005) ("Individuals who hitherto had no significant ties to radical organizations are enlisting themselves in the struggle and committing acts of violence, *sometimes without any support from existing networks*." (emphasis added) *id.* at xiii.) *See also* ANONYMOUS, *supra* note 35 at xii ("[T]he United States can no longer rely on its continental breadth, friendly neighbors, and broad oceanic shores to insulate it from [terrorist attack].").

As described below, these challenges are particularly acute for electronic surveillance in global communications systems where rules based on geographically-determined jurisdiction and the physical location of information infrastructure to be targeted are undermined by the global nature of the infrastructure and information flows, and rules based on indeterminate or arbitrary[37] attributes, such as citizenship, are technically impossible to enforce.

III. THE EAR OF DIONYSUS

The Ear of Dionysus (*L'Orecchio di Dionigi*) is the name given by the belligerently Baroque painter Caravaggio (1571-1610)[38] to a cave in Syracuse in which, legend has it, Dionysus[39] took advantage of the perfect natural acoustics that allowed eavesdropping on all conversations from one central spot.[40] *Ear of Dionysius* has come to generically refer to any structure in which the acoustic architecture naturally allows conversations to be heard surreptitiously at a distance—so, too, then, the global communication infrastructure.

A. FISA IS INADEQUATE

In addition to the general challenges detailed in the earlier section relating to preemption and the changed nature of the threat, FISA is inadequate as currently constituted in particular because it did not anticipate the development of global communication networks or advanced technical methods for intelligence gathering. Thus, it fails in practice to accommodate three specific circumstances:

---

[37] Here we mean *arbitrary* in a technical sense, that is, these attributes are unrelated to, or not obvious from, the data itself.

[38] Michelangelo Merisi da Caravaggio (b. Sep. 29, 1571 – d. Jul. 18, 1610) was an Italian artist considered the first great representative of the Baroque school. That he was belligerent is evidenced by a contemporary source: "[A]fter two weeks of work [Caravaggio] will sally forth for two months together with his rapier at his side and his servant-boy after him, going from one tennis court to another, always ready to argue or fight, so that he is impossible to get along with." CAREL VAN MANDER, HET SCHILDER-BOEK (1604), *translated in* HOWARD HIBBARD, CARAVAGGIO 344 (1985).

[39] Dionysus, the bastard son of Zeus and the mortal Semele, was the mythic god of fertility, wine, intoxication, and creative ecstasy. It was Dionysus who granted Midas the golden touch, then was benignant enough to relieve him of the power when it proved inconvenient. *See generally* ROBERT GRAVES, THE GREEK MYTHS AT 103-110, 281-282 (1960).

[40] Dorte Zbikowski, *The Listening Ear: Phenomena of Acoustic Surveillance* in CTRL [SPACE]: RHETORICS OF SURVEILLANCE FROM BENTHAM TO BIG BROTHER 38 (Thomas Y. Levin, *et al.* eds., 2002).

- First, because FISA has been interpreted by some to require a warrant for any electronic surveillance that "occurs in the United States" if there is a substantial likelihood of intercepting contents of a communication "to or from a person in the United States" it unnecessarily constrains surveillance of wholly foreign communications—say a phone call between an al Qa'ida safe house in Pakistan and a known terrorist financier in Indonesia—if the interception is physically accomplished at a telecommunications switch on U.S. soil while the communication is in transit ("transit intercepts").[41]

- Second, FISA provides a cumbersome binary mechanism requiring individual application to the FISA court for authorization to target a specific U.S. person or source based on showing probable cause of a connection to a foreign power or terrorist organization prior to any electronic surveillance, even in circumstances where collateral intercepts incidental to an authorized foreign intelligence target not subject to FISA might indicate reasonable suspicion that would require follow up surveillance or investigation to determine whether probable cause exists ("collateral intercepts"),[42] and

- Third, FISA does not provide any mechanism for programmatic pre-approval of technical methods like automated data analysis or filtering that may be the very method necessary for uncovering the connection to a foreign terrorist organization or activity in the first place ("automated analysis").

---

[41] *See* 50 U.S.C. § 1801 (f)(2) (2006); Eric Lichtblau & James Risen, *Domestic Surveillance: The Program; Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 24, 2005, at A6:

> One issue of concern to the [FISC] ... is whether the court has legal authority over calls outside the United States that happen to pass through American-based telephonic "switches."
>
> . . .
>
> Now that foreign calls were being routed through switches on American soil, some judges and law enforcement officials regarded eavesdropping on those calls as a possible violation of those decades-old restrictions, including the [FISA], which requires court-approved warrants for domestic surveillance.

see also note 42 *infra*.

[42] There is also a narrower but related problem where the incidental interception of international calls to or from the United States by a foreign surveillance target not normally subject to FISA are themselves viewed as triggering the warrant requirements of 50 U.S.C. § 1801(f)(2) when the interception is physically conducted from a switch in (thus, "occurs in") the U.S. It is believed that this was among the initial problems with FISA that lead to the Presidential authorization of the TSP, *see infra* text accompanying notes 54-61.

To understand why FISA is inadequate in these circumstances requires in part an understanding of the nature of modern communications networks.

B. TRANSIT INTERCEPTS: FROM CIRCUIT-BASED TO PACKET-BASED COMMUNICATION NETWORKS

The fundamental architecture of modern communications networks has changed significantly since FISA was enacted requiring new methods to conduct electronic surveillance. These developments challenge existing constructs underlying electronic surveillance law and policy.

> Thirty years ago when FISA was being drafted it made sense to speak exclusively about the interception of a targeted communication—one in which there were usually two known ends and a dedicated ("circuit-based") communication channel that could be "tapped." In modern networks, however, data and ... [digital] voice communications are broken up into discrete packets that travel along independent routes between point of origin and destination where these fragments are then reassembled into the original whole message. Not only is there no longer a dedicated circuit, but individual packets from the same communication may take completely different paths to their destination.[43]

---

[43] K. A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance,* N.Y.U. REV. L. & SECURITY, NO. VII SUPL. BULL. ON L. & SEC.: THE NSA AND THE WAR ON TERROR (Spring 2006) (hereinafter "*Whispering Wires*") *available at* http://whisperingwires.info. The NSA itself has described these developments:

> In the past, NSA operated in a mostly analog world of point-to-point communications carried along discrete, dedicated voice channels. ... Now, communications are mostly digital, carry billions of bits of data, and contain voice, data and multimedia. They are dynamically routed, globally networked and pass over traditional communications means such as microwave or satellite less and less. Today, there are fiber optic and high-speed wire-line networks and most importantly, an emerging wireless environment that includes cellular phones, Personal Digital Assistants and computers. ... The volumes and routing of data make finding and processing nuggets of intelligence information more difficult. ... The volume, velocity and variety of information today demands [sic] a fresh approach to the way NSA has traditionally done business. ... NSA's existing authorities were crafted for the world of the mid to late 20th Century, not for the 21st Century. ... [Because of this new] communications environment ... availability of critical foreign intelligence information will mean gaining access in new places and in new ways.

NATIONAL SECURITY AGENCY & CENTRAL SECURITY SERVICE, TRANSITION 2001 at 31-32 (Dec. 2000), *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa25.pdf.

In these "packet-based" networks, computerized switches ("routers") determine in real time and at various points along the way the most efficient route for ongoing packet traffic to take depending on current availability and congestion on the network, not simply on the shortest distance between two points. "Such random global route selection means that the switches carrying calls from Cleveland to Chicago, for example, may also be carrying calls from Islamabad to Jakarta."[44] To intercept these kinds of communications, filters ("packet-sniffers")[45] and search strategies[46] are deployed at various communication nodes (i.e., switches) to scan and filter all passing traffic with the hope of finding and extracting those packets of interest and reassembling them into a coherent message. Even targeting a specific message from a known sender may require scanning and filtering the entire communication flow at multiple nodes.[47]

---

[44] JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 50 (2006)

[45] A packet sniffer (a network diagnostic tool also known as a network analyzer) is computer software or hardware that can intercept and log traffic passing over a digital network or part of a network. As data travels over the monitored network segment, the sniffer can log each packet: an unfiltered sniffer captures all passing traffic and a filtered sniffer captures only those packets containing a specified data element. Captured packets must then be decoded, analyzed, and reassembled into a coherent message. For a readable technical discussion of sniffers, see SUMIT DHAR, SNIFFERS: BASICS AND DETECTION [v. 1.0-1] (2002), *available at* http://www.rootshell.be/~dhar/downloads/Sniffers.pdf.

[46] Because packets that are part of the same communication can travel different routes, or because their point of origin or destination can be masked using certain proxy routing techniques, search strategies covering multiple nodes (or covering multiple entry and exit points on proxy networks) may be needed to effectively intercept any particular communication. For a general discussion of proxy routing, including "mix networks" such as TOR that use "onion routing," see, Marc Rennhard & Bernhard Plattner, *Practical Anonymity for the Masses with Mix-Networks*, WETICE 255 (Twelfth International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003).

[47] A familiar example of a packet sniffing application for electronic surveillance was the Federal Bureau of Investigation's DCS-1000 application for lawful intercepts of email traffic (*aka* "Carnivore") (the FBI no longer uses DCS-1000, relying instead on commercial applications and the in house capabilities of Internet service providers for lawful intercepts). The DCS-1000 was intended to scan email traffic and only pick out and log material that was authorized under the particular search warrant pursuant to which it was being employed. *See Carnivore Diagnostic Tool, Testimony of Donald M. Kerr, Assistant Director, Laboratory Division, Federal Bureau of Investigation, before the U.S. Senate Committee on the Judiciary* (Sep. 6, 2000). Although certain details of the DCS-1000 remain classified, declassified documents describe a single-purpose Windows 2000/NT computer employing the DragonWare software suite, including: Carnivore, an analytic filter packet sniffer to capture packets; Packeteer, an application to reassemble packets into coherent messages, and Coolminer, an analytic tool to help analyze the intercepted data. *See* Kevin Poulsen, *Carnivore Details Emerge*, SECURITYFOCUS, Oct. 4, 2000. The use of DCS-1000 in practice highlights the very problem discussed in this article—it is increasingly technically difficult—maybe impossible—to intercept only targeted communications in a packet-based communications network. For example, according to an internal FBI memo, technicians threw out lawfully collected wiretap

Further, with the globalization of the telecommunications industry in recent years and the dominance of U.S. infrastructure providers, a large volume of international-to-international voice and email traffic is now routed through switches in the United States. A voice call from Europe to Asia, for example, may routinely go through a switch in the United States, and much of the world's email traffic—even messages sent between regionally neighboring states, say Pakistan and Sudan—may now pass through switches in the United States.[48] In addition, a significant amount of web content and email is hosted on U.S.-based servers. The growth of this 'transit traffic' is problematic for foreign intelligence surveillance because if FISA were to be applied strictly according to its terms prior to any electronic surveillance of communication flows where the acquisition occurs in the U.S. or there is a substantial likelihood of intercepting "U.S. persons" communications (since domestic U.S. traffic transits the same switches), then no electronic surveillance of any kind could occur anywhere

---

information from an investigation of Osama bin Laden's terrorist network when the DCS application accidentally also intercepted and logged non-targeted communications. *Memo: FBI Destroyed Terrorism E-mails*, USA TODAY, Apr. 29, 2002, at A16.

It has recently been alleged that because of these technical limitations the FBI is now using a broader approach to lawful intercepts in which all traffic on a particular network segment is collected and then the data is 'filtered' after the fact to extract those messages subject to the particular warrant or court order. *See* Declan McCullagh, *FBI Turns to Broad New Wiretap Method*, CNET NEWS.COM , Jan. 30, 2007. Applicable law and policy simply must be updated to account for these technical realities and to incorporate procedures that recognize that technical limitations require new methods to accomplish appropriate and lawful uses.

Modern network diagnostic tools, such as the Narus STA 6400 semantic traffic analyzer, give intelligence and law enforcement agencies powerful capabilities to monitor communications network activity under appropriate circumstances. However, existing laws and procedures, including those in FISA, are inadequate to accommodate technical and operational needs for their lawful employ while still protecting privacy and civil liberties.

[48] It is rumored that it was a reluctance to disclose how much international traffic transited U.S. switches, among other things, that dissuaded the administration from asking Congress for amendments to FISA to address this particular problem and that then ultimately led to the secret authorization of the Terrorist Surveillance Program. Attorney General Alberto Gonzales has stated that the Bush administration chose not to ask Congress for an amendment to FISA to authorize such wiretaps explicitly because it would have been difficult to get such an amendment without compromising classified information relating to operational details. *See White House Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence* (Dec. 19, 2005), http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html; and *Remarks by Homeland Security Secretary Chertoff and Attorney General Gonzales on the USA PATRIOT Act* (Dec. 21, 2005), http://www.dhs.gov/xnews/speeches/speech_0265.shtm.

without a warrant and there is no procedure within FISA that would accommodate this need.[49]

C. COLLATERAL INTERCEPTS: THE GLOBALIZATION OF COMMUNICATIONS

Another problem—somewhat orthogonal to that presented by transit intercepts—also arises when FISA is triggered by foreign intelligence collection conducted against communications "to or from a person in the United States" or against "U.S. persons" in these globalized communication networks. Advances in information technology, the borderless nature of terrorist threats, and global communications that may travel on random paths across political borders has made place-of-collection and U.S. personhood an increasingly unworkable basis for controlling the collection of intelligence because it is in many cases no longer technically possible to determine exactly when a communication is taking place "to or from the United States" and no practical means exists to determine if a particular participant is a U.S. person or not until after further investigation.[50] "In

---

[49] *See generally*, RISEN, *supra* note 44 at 42-60 (discussing the perceived need to circumvent FISA procedures); and *see* Eric Lichtblau & James Risen, *supra* note 41:

> One issue of concern to the [FISC] . . . is whether the court has legal authority over calls outside the United States that happen to pass through American-based telephonic "switches" . . . "There was a lot of discussion about the switches" . . . the gateways through which much of the communications traffic flows.
>
> . . .
>
> The switches are some of the main arteries for moving voice and some Internet traffic into and out of the United States, and, with the globalization of the telecommunications industry in recent years, many international-to-international calls are also routed through such American switches.
>
> . . .
>
> The growth of that transit traffic had become a major issue for the intelligence community, officials say, because it had not been fully addressed by 1970's-era laws and regulations ... . Now that foreign calls were being routed through switches on American soil, some judges and law enforcement officials regarded eavesdropping on those calls as a possible violation of those decades-old restrictions, including the [FISA], which requires court-approved warrants for domestic surveillance.

But see note 61 *infra* (discussing the FISC orders and speculating about the use of anticipatory warrants to 'pre-approve' certain collateral surveillance).

[50] Place-of-collection and citizenship of persons involved in the communication are increasingly *arbitrary* (in a technical sense) attributes of the intercepted communication, that is, these attributes are not obviously apparent or discernable from the place of interception or even from the communication itself. Publicly available intelligence guidelines discussing traditional operational assumptions—for example, that intercepts abroad are assumed to not target U.S. persons and those within the United States are—seem outdated as well. That place of collection and U.S. person rules are increasingly

fact, it is now difficult to tell where the domestic telephone system ends and the international network begins."[51] FISA does not account for this.

Thus, where collateral U.S. person communications are intercepted incidental to a legitimate foreign intelligence intercept, there is no explicit way consistent with FISA as currently constituted to engage in follow up electronic surveillance to determine if probable cause exists to target that individual,[52] even though the collateral intercept itself may give rise to a constitutionally reasonable suspicion.[53]

Communications of a U.S. person (including those to or from the United States) acquired incidental to a lawful foreign interception would generally be subject to collection, retention, and dissemination procedures

---

unworkable for information sharing is discussed in MARKLE TASK FORCE ON NATIONAL SECURITY IN THE INFORMATION AGE THIRD REPORT, MOBILIZING INFORMATION TO PREVENT TERRORISM: ACCELERATING DEVELOPMENT OF A TRUSTED INFORMATION SHARING ENVIRONMENT 32-41 (2006) (advocating replacing place of collection and U.S. persons rules with an "authorized use" standard for information sharing).

[51] RISEN, *supra* note 44 at 50. Note also that one can now acquire and use from anywhere in the world a Voice over Internet Protocol ("VoIP") telephone that has a local telephone number assigned in any area or country code desired. Some Jihadist websites specializing in countermeasure tradecraft have suggested acquiring VoIP telephones with domestic U.S. telephone numbers precisely so as to make surveillance more difficult by appearing to be domestic or U.S. person protected communications even though the communication is in fact wholly foreign.

[52] Although FISA permits applications for warrants to be made up to 72 hours after the fact in certain limited emergency situations, 50 U.S.C. § 1805(f), these procedures do not address the collateral intercept problem discussed in this article or the TSP problem discussed in note 42 *supra* because they impose the same *a priori* requirements, that is, even in an 'emergency' situation FISA requires the Attorney General to determine *before* approving the surveillance that the "factual basis for issuance of an order under [FISA] to approve such surveillance exists," even in cases where additional investigation or surveillance might be needed to determine such (or, in cases of incidental communications to or from the U.S., where the communication itself could not be anticipated but triggers FISA).

[53] For an overview of the relevant Fourth Amendment probable cause and reasonable suspicion standards, see Congressional Research Service, Memorandum to the Senate Select Committee on Intelligence, Probable Cause, Reasonable Suspicion, and Reasonableness Standards in the Context of the Fourth Amendment and the Foreign Intelligence Surveillance Act (Jan. 30, 2006) ("... the [Supreme] Court has pointed out that probable cause is the description of a degree of probability that cannot be easily defined out of context." *id.* at CRS-2.) *See also Hearing on Modernizing the Foreign Intelligence Surveillance Act (FISA) before the U.S. House Permanent Select Committee on Intelligence,* 109th Cong. (2006) (testimony of Kim Taipale, Executive Director, Center for Advanced Studies in Sci. & Tech. Pol'y) (hereinafter, "*HPSCI Testimony*") (discussing general Fourth Amendment requirements at 7-10) ; Taipale, *Frankenstein, supra* note 7 at 202-17 ("Towards a Calculus of Reasonableness"); K. A. Taipale, *Why Can't We All Get Along? How Technology, Security, and Privacy can Co-exist in the Digital Age, in* CYBERCRIME: DIGITAL COPS IN A NETWORKED WORLD 151, at 171-78 (Jack Balkin, *et al., eds.*, 2007) (discussing reasonableness and due process).

consistent with Executive Order 12,333.[54] While such information ostensibly could be retained and disseminated according to intelligence guidelines if it amounted to foreign intelligence or counterintelligence, it could not in practice be the basis for a FISA warrant application if its foreign intelligence value was not apparent on its face (that is, if it required follow up investigation, additional surveillance, or sharing with other agencies for context) because it would be subject to minimization procedures that would prevent its further retention or dissemination. Further, if the collateral interception of a call to or from the U.S. occurred from a switch in the United States while conducting lawful foreign surveillance not otherwise subject to FISA, the incidental interception of that communication itself could be considered to trigger statutory FISA warrant requirements, thus, the collected information could not be used *even if it evidenced probable cause on its face* unless the original interception was somehow authorized.[55]

The problem is simply that FISA requirements are now being triggered by unanticipated circumstances for communications that were not originally intended to be subject to FISA (that is, those incidental to a legitimate foreign target intercept) because, among other things, the capability to do foreign intercepts from within the United States is now technically feasible (and was not anticipated at the time FISA was enacted).

The untenable result in this particular case is that if the NSA were lawfully targeting a foreign source communicating with someone in the United States by monitoring a foreign switch, then that collateral communication would not be subject to FISA and might subsequently be used in support of an application for targeting the U.S. person or source. However, if that same surveillance was being conducted at a switch in the United States, any information from the collateral intercept could not be used in any manner (including especially for an application for a FISA warrant) if the incidental interception was deemed to have itself required a FISA warrant (because it occurred in the United States). Indeed, it appears that this specific "bootstrapping" problem was a particular concern of the FISC.[56]

Further, this problem could not simply be avoided by getting a FISA warrant for the original interception because it is uncertain whether the

---

[54] *See* note 15 *supra* and the referenced guideline documents.

[55] *See* 50 U.S.C. §1801 (f) (2000): "Electronic surveillance means: ... (2) the acquisition ... of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, *if such acquisition occurs in the United States*, ..." (emphasis added).

[56] *See* Carol D. Leonnig, *Surveillance Court is Seeking Answers*, WASH. POST, Jan. 5, 2006, at A2 ("[the presiding FISC judge] had ... raised concerns ... about the risk that the government could taint the integrity of the [FISC's] work by using information it gained via wiretapping [pursuant to Presidential authority under the TSP] to obtain warrants ... under the Foreign Intelligence Surveillance Act.").

FISC even has (or should have) jurisdiction[57] over the surveillance of a purely foreign target and it could not be known *a priori* that a communication to or from the U.S. would take place or with whom (thus, it would be impossible in practice to meet the requirements to support a traditional FISA warrant application). Obviously, even if there were FISC jurisdiction, it would be impractical to obtain warrants covering all foreign intelligence targets on the supposition that they might initiate or receive a communication from within the United States.[58]

As described in media reports, it appears that the Terrorist Surveillance Program (TSP) was specifically intended to address a particular aspect of the collateral intercept problem—that is, to authorize surveillance of collateral communications to and from the U.S. intercepted incidental to legitimate foreign surveillance activity without a FISA warrant even where FISA statutory requirements might otherwise be triggered (for example, where the interception was physically conducted at a U.S. switch thus triggering § 1801(f)(2)). According to official statements, the TSP authorized interception of international communications under presidential authority where one party to the communication was a legitimate target of foreign intelligence surveillance even if the other party was in the United States or a U.S. person.[59] Such surveillance previously authorized under the TSP is now subject to the FISC orders:

> I am writing to inform you that on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization.[60]

---

[57] For a general discussion of the creation, membership, structure and jurisdiction of the FISC and FISCR, see CONGRESSIONAL RESEARCH SERVICE, THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW, (Congressional Research Service No. RL33833, Jan. 24, 2007).

[58] Note, however, that it may be precisely these circumstances that the FISC orders address through use of "anticipatory" warrants. *See* note 61 *infra*.

[59] Attorney General Gonzales has stated that: "the standard applied [in the NSA Terrorist Surveillance Program under Presidential authority]—'reasonable basis to believe' [that one party to the communication was 'terrorist']—is essentially the same as the traditional Fourth Amendment probable cause standard." Attorney General Alberto R. Gonzales, *Prepared Remarks at the Georgetown University Law Center* (Jan. 24, 2006), http://www.usdoj.gov/ag/speeches/2006/ag_speech_0601241.html, and, further, specifically stated that the current FISC orders are based on "probable cause" to believe that "one of the communicants is [a 'terrorist']." *See* Gonzales letter, *supra* note 2 and Transcript, *infra* note 82.

[60] Attorney General's letter, *supra* note 2.

It is unlikely that the original TSP or the new FISC orders cover the entirety of the collateral intercept problem discussed in this article, but, in any case, FISA should be amended to provide an explicit statutory basis for these orders.[61]

D. AUTOMATED ANALYSIS: CONTENT FILTERING, TRAFFIC ANALYSIS, AND LINK OR PATTERN ANALYSIS[62]

> Automated screening can monitor data flows to uncover terrorist connections or terrorist communication channels without human beings ever looking at anybody's emails or listening in on their phone calls. Only when the computer identifies suspicious connections or information do humans get involved.[63]

It is beyond the scope of this article to explore all the different analysis techniques that can be applied to the automated monitoring of terrorist communications but three generic examples show the range of activity possible: *content filtering*, *traffic analysis*, and *pattern or link analysis*.

Content filtering is used to search for the occurrence of particular words or language combinations that may be indicative of particular

---

[61] Details of the FISC orders have not been publicly disclosed and the Justice Department has indicated that it is not prepared to release the orders to the public, *see* Government's Supplemental Submission, *supra* note 9 at 20 ("the longstanding practice is that FISA Court orders remain classified and not subject to public dissemination because, among other things, publication of FISA Court orders would notify the enemy of our targets and means of conducting surveillance"). Speculation about the nature of the FISC orders has included discussion of whether they take the form of "anticipatory warrants" that would authorize surveillance in the future if certain factual predicates were to occur. Anticipatory warrants would require a judge to agree ahead of time that if certain facts were to occur at some point in the future (for example, if a legitimate foreign target were to communicate to or from the United States), then probable cause would exist at that time to justify surveillance and electronic monitoring would be authorized and could be carried out under the warrant. The use of anticipatory warrants was upheld in U.S. v. Grubbs, 126 S. Ct. 1494, 1500 (2006) (warrant containing "triggering conditions" is constitutional). Although the use of anticipatory warrants to authorize collateral intercepts in these circumstances would mitigate some aspects of the collateral intercept problem discussed in this article, an explicit statutory basis should be enacted to support such orders. On Feb. 27, 2007, the Electronic Frontier Foundation filed a Freedom of Information Act request seeking release of Department of Justice records relating to the FISC orders. EFF v. Department of Justice, No. 07-CV-00403 (D. D.C., filed Feb. 27, 2007).

[62] Parts of this subsection are adapted from Taipale, *Whispering Wires*, *supra* note 43.

[63] K. A. Taipale & James Jay Carafano, *Fixing Foreign Intelligence Surveillance*, WASH. TIMES, Jan. 25, 2006, at A15.

communications (or persons) of interest.[64] A simple example of this would be to screen for messages to or from known terrorist sources containing the words "nuclear weapon" or "osama bin laden." Actual search algorithms are, of course, much more complex and sophisticated and can employ artificial intelligence, machine learning, and powerful statistical methods such as Bayesian analysis to identify "signals of interest." It should be made clear that the filtering contemplated here is not the same as undirected "data mining" in which all communication flows are screened looking for previously unknown general indicia of suspicion with no starting point.[65]

Traffic analysis is the observation of traffic patterns—message lengths, frequency, paths, etc.—of communications without examining the content of the message (traffic analysis can be used even where content is encrypted).[66] Traffic analysis can reveal patterns of organization, for example, by measuring "betweeness" in email traffic[67] or other communications among known or suspected terrorists or terrorist communication channels or networks. By looking for patterns in traffic these techniques, together with analytical methods such as social network theory, can identify organizations or groups and the key people in them.[68]

---

[64] For example, the Echelon program has been described as an NSA program (in partnership with corresponding agencies in Australia, Canada, New Zealand, and the UK) to automatically filter and sort intercepted foreign communications using "dictionaries" consisting of targeted keywords—names, addresses, telephone numbers, IP addresses, aliases, affiliates, etc.—for different categories of targets. PATRICK RADDEN KEEFE, CHATTER 116 (2006). The existence of Echelon has not been officially acknowledged and the details of the program are classified. However, most public accounts describe a process in which communications are flagged by certain keywords. *See, e.g.*, Federation of American Scientists Web Site, http://www.fas.org/irp/program/process/echelon.htm; European Parliament, Temporary Committee on the ECHELON Interception System, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)* (2001/2098-INI) (Jul. 11, 2001). And, see U.S. Patent 6,169,969 for a "device and method for full-text large dictionary string matching" discussed in Keefe, *supra* at 121-22.

[65] See discussion of link and pattern analysis below.

[66] *See* BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD 34-35 (2000) ("Traffic analysis is the study of communication patterns ... [o]ften the patterns of communication are just as important as the contents of communications").

[67] Links with high "betweenness" are those infrequently used links that connect groups from two distinct communities of frequently connected individuals. *See generally* Linton C. Freeman. *A Set of Measures of Centrality Based on Betweenness*, 40 SOCIOMETRY, Mar. 1977, at 35–41.

[68] Covert social networks exhibit certain characteristics that can be identified. *Post hoc* analysis of the 9/11 terror network shows that these relational networks exist and can be identified, at least after the fact. Vladis E. Krebs, *Uncloaking Terrorist Networks*, 7 FIRST MONDAY, April 2002 (mapping and analyzing the relational network among the 9/11 hijackers). Research on mafia and drug smuggling networks show characteristics particular to each kind of organization, and current social network research in counterterrorism is focused on identifying unique characteristics of terror networks. *See generally* Philip Vos Fellman & Roxana Wright, *Modeling Terrorist Networks: Complex Systems at the Mid-*

These methods can uncover how terrorist groups are organized and reveal activity even if they are communicating in code or only discussing the weather.[69]

Link or pattern analysis in this context is the use of observed or hypothesized connections or patterns to find other related but unknown relationships. Again, it is important to distinguish undirected "data mining" for general patterns of suspicion from the targeted use of pattern matching to allocate investigative resources being discussed here.[70]

For example, known patterns of terrorist communications can be identified and used to uncover other unknown but indirectly related terrorists. Thus, for instance, in the immediate aftermath of 9/11 the FBI determined that the leaders of the nineteen hijackers had made 206 international telephone calls to locations in Saudi Arabia, Syria, and Germany.[71] It is believed that in order to determine whether any other

---

Range, presented at Complexity, Ethics and Creativity Conference, London School of Economics (Sep. 17-18 2003); Joerg Raab & H. Briton Milward, *Dark Networks as Problems*, 13 J. OF PUB. ADMIN. RES. & THEORY 413-39 (2003); Matthew Dombroski *et al.*, *Estimating the Shape of Covert Networks*, PROCEEDINGS OF THE 8TH INT'L COMMAND AND CONTROL RES. AND TECH. SYMPOSIUM (2003); H. Brinton Milward & Joerg Raab, *Dark Networks as Problems Revisited: Adaptation and Transformation of Islamic Terror Organizations since 9/11*, presented at the 8th Publ. Mgt. Res. Conference at the School of Policy, Planning and Development at University of Southern California, Los Angeles (Sep. 29-Oct. 1, 2005); D. B. Skillicorn, *Social Network Analysis Via Matrix Decomposition*, in EMERGENT INFORMATION TECHNOLOGIES AND ENABLING POLICIES FOR COUNTER TERRORISM (Robert Popp and John Yen, *eds.*, Jun. 2006). For a general overview of global Salafi jihadist terror networks, *see* Marc Sageman, UNDERSTANDING TERROR NETWORKS (2004).

[69] *See, e.g.*, Hazel Muir, *Email Traffic Patterns can Reveal Ringleaders*, NEW SCIENTIST, Mar. 27, 2003. For a general discussion of the use of social network theory in counterterrorism analysis, see Patrick Radden Keefe, *Can Network Theory Thwart Terrorists?*, N.Y. TIMES MAGAZINE, Mar. 12, 2006, at 16.

[70] It is beyond the scope of this article to discuss general data mining issues in greater detail. For a detailed discussion of these and related issues, *see* K. A. Taipale, *Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data*, 5 COLUM. SCI. & TECH. L. REV. 2 (2003) (hereinafter, *Connecting the Dots*). For a detailed rebuttal of popular arguments against the potential usefulness of data mining for counterterrorism applications, see *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before U.S. Senate Judiciary Committee*, 110th Cong., at 6-16 (Jan. 10, 2007) (testimony of Kim Taipale, Executive Director, Center for Advanced Studies in Sci. & Tech. Pol'y) ("Popular arguments about why [data mining] won't work for counterterrorism are simply wrong – . . . the commercial analogy is irrelevant, the 'training set' problem is a red herring, and the false positive problem can be significantly reduced by using appropriate architectures—and, in any case, is not unique to data mining.").

[71] John Crewdson, *Germany says 9/11 hijackers called Syria, Saudi Arabia*, CHI. TRIB., Mar. 8, 2006, at C17 ("According to [a classified report based on telephone records obtained from the FBI], 206 international telephone calls were known to have been made by the leaders of the hijacking plot after they arrived in the United States—including 29 to Germany, 32 to Saudi Arabia and 66 to Syria.").

unknown persons—so-called sleeper cells—in the United States might have been in communication with the same pattern of foreign phone numbers[72] the NSA analyzed Call Data Records (CDRs) of international and domestic phone calls obtained from the major telecommunication companies. [73] Undertaking such an analysis seems reasonable, particularly in the circumstances immediately following 9/11, yet, FISA and existing procedures do not provided an authorizing mechanism for determining such reasonableness because FISA simply did not contemplate the need for approval of specific—but not individualized—pattern-based data searches or surveillance.[74]

It is important to point out again that the kind of automated analysis being discussed in this section is not the undirected "data mining" to look for general indicia of "suspicious behavior" that rightly has libertarians[75]

---

[72] That is, to uncover others who may not have a direct connection to the nineteen known hijackers but who may exhibit the same or similar *patterns of communication* as the known hijackers.

[73] That the NSA obtained CDRs from U.S. telecommunication carriers for analysis was implied in Lichtblau, *supra* note 41, and was explicitly alleged in Cauley, *supra* note 2.

[74] FISA specifically includes procedures for use of so-called pen register or trap and trace devices to record addressing details from phone conversations under a lower standard than that required for content interception (i.e., lower than that required for "wiretaps"), 50 U.S.C. § 1842 (2000), however, it provides no mechanism for authorizing searches for specific traffic information from general databases.

It is settled law under *Smith v. Maryland*, 442 U.S. 735 (1979), that addressing information is generally entitled to lesser constitutional protection than communication content. *See generally* ELIZABETH B. BAZAN *ET AL.*, GOVERNMENT ACCESS TO PHONE CALLING ACTIVITY AND RELATED RECORDS: LEGAL AUTHORITIES 3-5, (Congressional Research Service Report to Congress No. RL33424, 2007). Further, the particularity requirement of the Fourth Amendment does not impose an irreducible requirement of individualized suspicion before a search can be found reasonable, or even to procure a warrant. In at least six cases, the Supreme Court has upheld the use of drug courier profiles as the basis to stop and subject individuals to further investigative actions, including search. *See, e.g.*, United States v. Sokolow, 490 U.S. 1 (1989); Steven K. Bernstein, *Fourth Amendment: Using the Drug Courier Profile to Fight the War on Drugs*, 80 J. CRIM. L. & CRIMINOLOGY 996 (1990). More relevant, the court in *United States v. Lopez*, 328 F. Supp 1077, 1092 (E.D.N.Y. 1971), upheld the validity of hijacker behavior profiling, opining that "in effect ... [the profiling] system itself ... acts as informer" serving as sufficient constitutional basis for initiating further investigative actions. Yet, FISA simply provides no mechanism to address the need for authorization in the described circumstances.

[75] *See, e.g.*, *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before the U.S. Senate Committee on the Judiciary*, 110th Cong. (Jan. 10, 2007) (testimony of Robert Barr, Chief Executive Officer, Liberty Strategies, LLC); and *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before the U.S. Senate Committee on the Judiciary*, 110th Cong. (Jan. 10, 2007) (testimony of Jim Harper, Director of Information Policy Studies, The Cato Institute).

and civil libertarians[76] concerned about fishing expeditions or general searches to examine all communication flows in the manner of a general warrant.[77] These automated monitoring technologies should not be employed as a general method for "finding terrorists" by screening all global communications with no starting point, nor should they be used for determining guilt or innocence.[78] Rather, they should be employed carefully—subject to appropriate authorizations and effective oversight—as powerful tools to help better allocate law enforcement and security resources to more likely targets.[79] As such, automated analysis is simply

---

[76] *See, e.g.*, *Hearing on Balancing Privacy and Security: The Privacy Implications of Government Data Mining Programs before the U.S. Senate Judiciary Committee*, 110th Cong. (Jan. 10, 2007) (statement of Leslie Harris, Executive Director, Center for Democracy & Technology); *see* JAY STANLEY & BARRY STEINHARDT, AMERICAN CIVIL LIBERTIES UNION, BIGGER MONSTER, WEAKER CHAINS: THE GROWTH OF AN AMERICAN SURVEILLANCE SOCIETY 11-12, (2003).

[77] *See, e.g.*, Taipale, *HPSCI Testimony*, *supra* note 53 at 5-6 ("*Programs of surveillance* are not general warrants"). It was the use of general warrants by the English that led in part to the American Revolution, *see, e.g.*, O.M. Dickerson, *Writs of Assistance as a Cause of the Revolution*, in THE ERA OF THE AMERICAN REVOLUTION 40-75 (Richard Morris ed., 1939), and to enactment of the Fourth Amendment, *see* EDWARD CORWIN, THE CONSTITUTION AND WHAT IT MEANS TODAY at 341 (1978, 1920); DAVID HUTCHINSON, THE FOUNDATIONS OF THE CONSTITUTION at 294-95 (1975, 1928); *and* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION at 51-105 (1937).

[78] See *Connecting the Dots*, supra note 70 at 19; and Paul Rosenzweig, *Proposals for Implementing the Terrorism Information Awareness System*, 2 GEO. J. L. & PUB. POL'Y 169, 190 (2004) (discussing the appropriate consequences of pattern-based identification).

[79] One of the criticisms of using predictive risk management techniques for counterterrorism is to suggest that these methods may cast a wide net of "suspicion" and that many of these "suspects" will be innocent. *See, e.g.*, Stanley & Steinhardt, *supra* note 76 at 12; JEFF JONAS & JIM HARPER, CATO INSTITUTE, EFFECTIVE COUNTERTERRORISM AND THE LIMITED ROLE OF PREDICTIVE DATA MINING 7 (December 11, 2006) (for a detailed critique of the many inductive fallacies in the Cato Institute paper, *see* Testimony, *supra* note 70). But such an assumption is not uncritically warranted as these simplistic arguments confuse the use of probability-based resource allocation for investigative purposes with the assignment or determination of guilt (that is, they confuse attention with a determinative inference of "suspicion").

For example, in the ordinary course of law enforcement, the use of statistical or trend analysis to assign resources—say more beat officers to a high crime neighborhood—does not automatically lead to the inference that everybody in that neighborhood is a suspect, only that assigning resources there may be more effective than assigning them elsewhere. So, too, in counterterrorism, computational analytic tools can help allocate intelligence and law enforcement resources more effectively so long as care is taken to design policy and systems to avoid automatically triggering adverse consequences—such as determining guilt or innocence or otherwise denying rights—without adequate opportunities for error correction and redress. *See also* K. A. Taipale, *The Trusted Systems Problem: Security Envelopes, Statistical Threat Analysis, and the Presumption of Innocence*, 20 IEEE INTELLIGENT SYSTEMS, Sept./Oct. 2005, at 80–83("[I]t is the probative value of the [analysis], rather than its probabilistic nature, that is relevant in determining

the computational automation of traditional investigative procedures: monitoring known or suspected terrorists, following links from these suspects, or looking for specific patterns of operations or behaviors (i.e., observing and anticipating *modus operandi*).

FISA as currently constituted is unworkable in the context of globalized communications networks and advanced technical methods for gathering intelligence because it provides no mechanisms to adequately address the authorization and oversight of transit intercepts, collateral intercepts, and the use of automated monitoring. Simply to insist that these problems be ignored and that FISA is adequate "as is" is to engage in policy-making in a dangerous state of denial reminiscent of King Ludd.[80] Likewise, seeking solution only in streamlining cumbersome procedures[81] is to address symptoms, not root causes. Nor is it appropriate as a matter of public policy to resolve the deficiencies through "innovative" interpretations of existing FISA provisions, particularly when such outcomes are negotiated in secret and enacted through undisclosed FISC orders.[82] What is needed, in my view, is a rethinking of foreign intelligence

---

whether it is a sufficient predicate for government action. To argue otherwise is to confuse the presumption of innocence with the probability of innocence." *id.* at 82).

[80] *See* Taipale, *Frankenstein*, at 126-27, 220-21 (arguing that the lesson to be drawn from the experience of the *luddites* is that simple opposition to technological change is doomed to failure and therefore adaptation is a better policy).

[81] For example, as proposed in the Lawful Intelligence and Surveillance of Terrorists in an Emergency by NSA Act ("LISTEN Act"), H.R. 5371, 109th Cong. (2006) (the Harman-Conyers bill) (providing tools to expedite emergency warrant applications and authorizing funds to incorporate standardization, electronic filing and streamlined review procedures at the NSA and DOJ for FISA warrant applications). These provisions are both laudable and necessary—but not alone sufficient. However, such procedural improvements should be included in any future legislation that also addresses the substantive failings of FISA as discussed in this article.

[82] The Attorney General has described the FISC orders as "innovative" and "complex" requiring two years of negotiations between the administration and the FISC:

> These orders are innovative, they are complex, and it took considerable time and work for the Government to develop the approach that was proposed to the Court and for the judge on the FISC to consider and approve these orders.

Letter of the Attorney General, *supra* note 2. And, in a background briefing by two "senior Justice Department officials":

> These orders, however, are orders that have taken a long time to put together, to work on. They're orders that take advantage of use of the use of the FISA statute and developments in the law. I can't really get into developments in the law before the FISA court. But it's a process that began nearly two years ago, and it's just now that the court has approved these orders.

Transcript of Background Briefing by Senior Justice Department Officials on FISA Authority of Electronic Surveillance (Jan. 17, 2007), *available at* http://www.fas.org/irp/news/2007/01/doj011707.html.

surveillance that takes into account the changed security and technology context and a careful updating and amending of FISA and related procedures to specifically meet these challenges—including, if appropriate, an explicit statutory basis for the existing FISC orders—while still upholding core constitutional principles.[83]

IV. FIXING FOREIGN INTELLIGENCE SURVEILLANCE

To address the deficiencies identified in the previous section, FISA should be amended to provide for:

1. explicit authority or programmatic pre-approval[84] without requiring individual warrants for *transit intercepts*, that is, intercepts "at the

---

But, "[t]he legality of this ... surveillance program should not be decided by a secret court in one-sided proceedings." Press Release, American Civil Liberties Union, ACLU Demands More Information on "Innovative" Orders Issued by Secret Court, (Jan. 17, 2007). For speculation about the nature of the FISC orders, *see* note 61 *supra*.

[83] Despite the issuance of the FISC orders now authorizing surveillance previously authorized under the TSP, the administration also still believes that FISA needs updating:

> [W]e in the administration continue to believe that Congress should enact FISA reform legislation to modernize FISA statute to reestablish what we think is the proper, original focus of FISA on the domestic communications of U.S. persons. We believe that debate should continue to happen, that Congress should consider modernizing FISA very quickly in the new Congress.

Transcript, *supra* note 82.

[84] It is beyond the scope of this article to recommend particular mechanisms or standards for authorizing programmatic or other approvals. It has been argued that courts are ill-suited, and may be constitutionally prohibited, from such an oversight role, *see, e.g.*, David B. Rivkin, Jr. & Lee A. Casey, *Commentary: Inherent Authority*, WALL ST. J., Feb. 8, 2006, at A16 ("The federal courts can only adjudicate actual cases and controversies; they cannot offer advisory opinions"), and that a statutory executive or legislative authorization or oversight body should be created. Compare, for example, the proposed Terrorist Surveillance Act of 2006, S. 3931, 109th Cong. (2006) (the DeWine bill) that would approve the Terrorist Surveillance Program subject to oversight by special Congressional committees with the proposed National Security Surveillance Act of 2006, S. 3876, 109th Cong. (2006) (the Specter bill) that would require FISA court (FISC) approval and oversight, including review every forty-five days to continue "electronic surveillance programs." *See also*, Taipale, *HPSCI Testimony, supra* note 53 at 10-12 (discussing the pros-and-cons of judicial versus legislative involvement); and *see* John Schmidt, *Together Against Terror*, LEGALTIMES, Jan. 15, 2007 (arguing persuasively for a legal structure that involves the courts in order to foster the necessary confidence in the legality of the surveillance activity). *Cf.* Electronic Surveillance Modernization Act, H.R. 5825, 109th Cong. (2006) (the Wilson bill) (passed by the House on Sep. 28, 2006 and referred to the Senate Committee on the Judiciary) (requiring Congressional oversight but allow submission of the TSP to the FISC for review).

Although the exact scope of the current FISC orders has not been disclosed, the administration has denied that they are "programmatic" in the advisory sense:

switch" aimed at foreign communications but that might currently trigger statutory FISA warrant requirements[85] because the acquisition "occurs in the U.S." (or elsewhere with the "likelihood that the surveillance will [also] acquire the contents of any communication to which a United States person is a party"),

2. programmatic pre-approval[86] without requiring individual warrants of *automated analysis* and monitoring methods, including targeted content filtering, traffic analysis, and link or pattern analysis in specific contexts where the initial target or channel is a legitimate foreign intelligence target but the surveillance takes place within the U.S. or there is a likelihood of intercepting U.S. persons,[87] and

3. the statutory equivalent of a *Terry* stop[88] to permit limited follow up electronic surveillance of suspicious communications, including those involving U.S. persons, *collaterally intercepted* incidental to an authorized surveillance (including incidental to those authorized through programmatic approval under (1) and (2) above).

> I will say that these are not – these orders are not some sort of advisory opinion ruling on the program as a whole. These are orders that comply with the terms and requirements of the FISA statute, just like other orders issued by the FISA court.

Transcript, *supra* note 82. Thus, it has been speculated that the orders are more in the nature of anticipatory warrants, *see* note 61 *supra*, that authorize surveillance when or if certain circumstantial facts that would amount to probable cause occur in the future. *See, e.g.*, *How Do Innovative Spy Warrants Work? One Expert Speculates*, WIRED News, Jan. 22, 2007, at 27B.

[85] Note that these are statutory warrant requirements, not Constitutionally requirements. *See* Taipale, *HPSCI Testimony*, *supra* note 53 at 8-9 (discussing warrant requirements). As discussed in note 15 *supra*, even under the stricter standard of Title III, the Supreme Court has repeatedly held that warrantless interceptions collateral to a lawful intercept are not violations of the Fourth Amendment.

[86] *See supra* note 84.

[87] Note that under some intelligence collection guidelines, electronic data is generally not considered "collected" until it has been processed into intelligible form. *See, e.g.*, Department of Defense Directive 5240.1-R *Procedures Governing the Activities of DoD Intelligence Components that Affect U.S. Persons* at 15 §C2.2.1 (1982). Thus, bringing automated analysis under a statutory scheme might actually provide more oversight for some activity than under current guidelines.

[88] Terry v. Ohio, 392 U.S. 1 (1968) (holding that a police officer may stop an individual on the basis of "reasonable suspicion" and conduct a limited follow up search prior to establishing probable cause).

It is beyond the scope of this article to examine the related constitutional jurisprudence in detail.[89] However, there is likely no constitutional prohibition to a carefully crafted legislative solution that would statutorily authorize programmatic approval of electronic surveillance programs for foreign intelligence purposes that (i) target foreign communications transiting the U.S. or (ii) use automated analysis or monitoring methods, and which would also authorize limited follow-up investigation or surveillance based on reasonable suspicion of U.S. persons initially identified through collateral intercepts in order to determine if probable cause sufficient to meet FISA requirements for a warrant could be established.[90]

Further, permitting such programs may actually be preferable—and, ultimately, less intrusive to civil liberties—than alternative methods, for example, requiring physical surveillance to independently establish probable cause following a determination of reasonable suspicion incidental to a legitimate foreign intelligence intercept.

What is needed is an explicit statutory mechanism, incorporating the necessary democratic checks-and-balances, for programmatic approval of transit intercepts and automated analysis targeted against known or reasonably suspected foreign terrorist communication sources—that is, against legitimate foreign intelligence targets normally not subject to FISA and normally not requiring a warrant—even where such surveillance or technical methods may "occur in the United States" or where there is a likelihood of intercepting U.S. persons communications. If the initial process identifies potentially suspicious connections to or from legitimate foreign intelligence targets—including, for example, U.S. persons or

---

[89] For a detailed discussion of the Constitutional issues involved, *see* references in note 53 *supra;* and RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY (2006).

[90] Note that with regard to the TSP, Attorney General Gonzales has stated that: "the standard applied—'reasonable basis to believe'—is essentially the same as the traditional Fourth Amendment probable cause standard." Gonzales, *supra* note 59. And, further, that the current FISC orders are based on "probable cause." *See* Gonzales letter, *supra* note 2 and Transcript, *supra* note 82. For an overview of the Fourth Amendment probable cause and reasonable suspicion standards, *see* Congressional Research Service Memorandum to the Senate Select Committee on Intelligence, *supra* note 53 at CRS-2 ("... the [Supreme] Court has pointed out that probable cause is the description of a degree of probability that cannot be easily defined out of context.").

Thus, there are two related issues involved here: first, whether there are actually two standards—reasonable suspicion and probable cause; and, second, who—a FISC judge following lengthy *a priori* FISA procedures (or *ad hoc* anticipatory procedures, see note 61 *supra*) or a "shift-supervisor" [senior intelligence officer] at the NSA in "hot pursuit" of an intercepted communication—makes the determination. A statutory *Terry*-like procedure would address both by leaving some discretion with the "officer on the scene" (consistent with *Terry*) but subject to explicit statutory procedures and the Constitutional standard of reasonableness.

sources communicating with known or suspected terrorists or through known or suspected terrorist communication channels—then some additional appropriately authorized monitoring or follow-up investigation (including technical analysis, monitoring, or additional circumscribed electronic surveillance) should be permitted in order to determine if that initial "reasonable suspicion" is justified.[91]

---

[91] Incidental intercepts of U.S. person data are subject to minimization procedures that in practice restrict effective use of such collateral information unless it has foreign intelligence or counterintelligence (or in some cases, criminal intelligence) value on its face. Use, retention or dissemination of such information is restricted by minimization guidelines—for example, by blocking out the name or phone number of U.S. persons (*see, e.g.*, USSID 18 §6(b): "may be disseminated ... if the identity of the United States person is deleted and a generic term or symbol substituted so that the information cannot reasonably be connected with an identifiable United States person")—in a way that does not, in practice, permit it to be used to develop independent probable cause to target that U.S. person, particularly where its foreign intelligence value would only be apparent upon follow up investigation or dissemination. 50 U.S.C. § 1801 (h) (2000); *see* note 15 *supra* (Executive Order 12,333 and related guideline documents). (Prior to 9/11 such information was not even routinely shared with other government agencies and, in keeping with Attorney General guidelines, could not even be shared in practice within the FBI itself between the intelligence division and the criminal division. *See* Attorney General Janet Reno, Procedures for Contacts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations (Jul. 19, 1995). This latter problem was subsequently addressed in the Mar. 6, 2002 Attorney General guidelines, *Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI*.) And, as discussed in Section III (B) & (C) *supra*, in cases where the collateral intercept itself triggers FISA (because it "occurs in the United States," for example) such information cannot subsequently be used at all unless the original interception is specifically authorized. Indeed, it appears that concern specifically over the use of information from the TSP intercepts to establish probable cause for subsequent FISA warrant applications may have led to a three week suspension of the TSP in 2004. *See* Carol D. Leonnig, *Secret Court's Judges Were Warned About NSA Spy Data*, WASH. POST, Feb. 9, 2006. Thus, another way to deal with this particular aspect of the collateral intercept problem would be to change the statutory minimization procedures to explicitly permit some limited follow-up investigation or surveillance (along the lines suggested above under the *Terry* stop equivalent) and to explicitly sanction the use of information gleaned during this period (or otherwise collateral to a programmatic intercept) for subsequent warrant applications.

It should be noted that Attorney General Gonzales in his testimony to the Senate Judiciary Committee on Jan. 17, 2007 specifically mentioned that the FISC orders include minimization procedures "above and beyond" those typically required under the law. Thus, it can be speculated that through a combination of anticipatory warrants (*see* note 61 *supra*) and enhanced minimization procedures, the administration and the FISC (or at least one judge of the FISC) were able to agree a procedure that authorizes collateral intercepts and permits information from those intercepts to act as predicate for limited targeting of international communications. Information collected pursuant to those orders could then presumably serve as the basis for requesting a 'normal' FISA warrant to target the domestic end or U.S. person should probable cause be established (indeed, the predicate for such targeting may have been already been predetermined as part of the "anticipatory warrants,"

The problem with FISA is that it contemplates only a single binary *a priori* threshold for authorizing any electronic interception within the U.S. or involving U.S. persons — probable cause that the target is an agent of a foreign power.[92] Unfortunately, even extensive contact with a known terrorist may not be procedurally sufficient to satisfy the current requirements for a FISA warrant, yet such contact may have significant "foreign intelligence value" requiring follow up investigation (and would also meet the constitutional requirement of reasonableness).

Thus, what is needed, in my view, is a statutory basis for the electronic surveillance equivalent of a *Terry* stop, the constitutionally permissible procedure under which a police officer can briefly detain someone for questioning and conduct a limited pat-down search if they have 'reasonable suspicion' to believe that the person may be involved in a crime.[93] In the case of electronic surveillance, this would permit a circumscribed but authorized procedure for follow-up monitoring or investigation of initial suspicion derived from automated monitoring (or otherwise developed collateral to a legitimate foreign intelligence intercept).

If ongoing suspicion is not justified on follow-up analysis or surveillance, monitoring would be discontinued and normal (or enhanced[94]) minimization procedures would be triggered; however, if suspicion is reasonably justified then monitoring could continue under the programmatic approval for some limited further period to determine if standard statutory probable cause can be established. If there is probable cause to suspect that the target is actively engaged in terrorism or is an "agent" of a foreign

---

see note 61 *supra*). Again, the point of this article is to argue that FISA should be amended to provide an explicit statutory basis for these orders (or their equivalents).

[92] Assuming that the current FISC orders conform to the speculation regarding "anticipatory warrants," *see* note 61 *supra*, then what the administration and the FISC seem to have done is to have agreed a set of future factual circumstances that would amount to probable cause if (or when) they were to occur—that is, to anticipate that communications to or from a person in the United States with a legitimate foreign target may occur and to "pre-authorize" surveillance of those communications should they actually occur. While such a process might be shoehorned within the spirit and convoluted language of FISA, it would certainly have greater legitimacy—that is, a greater claim to be recognized as right and just, *see generally* Jurgen Habermas, COMMUNICATION AND THE EVOLUTION OF SOCIETY 178 (1976) (discussing "legitimacy")—if it were subject to explicit statutory authority and procedures. *See also* Schmidt, *supra* note 84 (arguing for legislation to explicitly extend the FISC jurisdiction to allow programmatic approval).

[93] *See* Taipale, *Whispering Wires*, *supra* note 43 (discussing the "electronic surveillance equivalent of a *Terry* stop").

[94] Normal minimization procedures are intended to limit retention or use of incidentally acquired U.S. person information without foreign intelligence value. A statutory regime that would permit collateral intercepts and sanction the use of collaterally collected information subject to programmatic approvals to establish independent predicate for additional warrants might require enhanced minimization procedures to isolate analysis and manage disposition of collateral information. As discussed in note 91 *supra*, it appears that the FISC orders include enhanced minimization procedures.

terrorist group, then a regular FISA warrant would be sought to target that U.S. person or source for full surveillance.

Based on published reports and public statements by intelligence officials responsible for the Terrorist Surveillance Program it is my belief that this indeed describes generally the procedures that the TSP was following,[95] and that are currently being authorized under the FISC orders.[96]

CONCLUSION

What is needed, then, is to provide a statutory mechanism that involves congressional authorization and oversight, together with an explicit statutory basis for judicial orders and review, so that legitimate foreign intelligence requirements can be met without resorting to unilateral secret executive branch approvals or by shoehorning "innovative" solutions not explicitly anticipated under FISA. Regardless of whether the President indeed currently has statutory or inherent authority to approve such programs, or whether a FISC judge can be convinced to stretch FISA to cover certain needs, our system of government works best, and public confidence is best maintained, only when the three branches of government work together in consensus and the broad parameters of procedural protections are publicly debated and agreed. Further, the ability of our government to respond appropriately to emergent national security threats is too important to be wholly dependant on the negotiation of ad hoc procedures during times of crises.

The central issue regarding foreign intelligence surveillance in modern communication systems is under what conditions information derived from collateral intercepts from legitimate surveillance of foreign intelligence targets or through automated monitoring can itself provide the reasonable predicate to allocate additional investigative resources for follow up investigation or surveillance even when it involves "U.S. persons" or when the communication takes place within the United States. FISA currently provides no workable mechanism for addressing these circumstances and should be amended.

---

[95] *See, e.g.*, Remarks by Gen. Michael V. Hayden, Principal Deputy Director Of National Intelligence and Former Director of the National Security Agency, *Address To The National Press Club: What American Intelligence & Especially The NSA Have Been Doing To Defend The Nation*, National Press Club, Washington, D.C. (Jan. 23, 2006). (Gen. Hayden was subsequently appointed Director of Central Intelligence on May 8, 2006, confirmed by the Senate on May 26, 2006, and sworn in May 30, 2006).

[96] *See generally* notes 2, 42, 61, 82, 84, 90, 91, and 92 *supra*.

○